

---

# Operational notes

Document updated on **June 23, 2022**.

The following colors are **not** part of the final product, but serve as highlights in the editing/review process:

- text that needs attention from the Subject Matter Experts: Mirco, Anna,& Jan
- terms that have not yet been defined in the book
- things that need to be checked only at the very final typesetting stage (and it doesn't make sense to do them before)
- text that needs advice from the communications/marketing team: Aaron & Shane
- text that needs to be completed or otherwise edited (by Sylvia)

















































# Todo list

12	■ Sylvia: This subsection should be in the introduction of the book as it applies to the	
13	entire math part . . . . .	12
14	■ zero-knowledge proofs . . . . .	12
15	■ add references . . . . .	12
16	■ Sylvia: This subsection should be in the introduction of the book as it applies to the	
17	entire math part . . . . .	13
18	■ Sylvia: We should put this table into the same introduction as 3.1.1 . . . . .	14
19	■ @jan @anna double check this definition. Is it clear enough? Proper definition re-	
20	quires the concept of equivalence or coprimeness first . . . . .	14
21	■ Do we even need this quantum computing excursion? . . . . .	16
22	■ @jan. You wrote: a and b are required to be non-zero in the definition above, so this	
23	can just be deleted. ... a can be zero and existence and uniqueness, non-zeroness	
24	are not obvious. Do you mean something else? . . . . .	16
25	■ You wrote: if these should only satisfy the equation, why use definition symbols	
26	(:=) and not equality symbols (=)? But this is a definition the symbol a div b IS	
27	DEFINED to be the number b... Is that clear? . . . . .	17
28	■ check algorithm floating . . . . .	24
29	■ subtrahend . . . . .	34
30	■ minuend . . . . .	34
31	■ algorithm-floating . . . . .	35
32	■ check algorithm floating . . . . .	38
33	■ Sylvia: I would like to have a separate counter for definitions . . . . .	41
34	■ check reference . . . . .	47
35	■ runtime complexity . . . . .	47
36	■ add reference . . . . .	47
37	■ S: what does “efficiently” mean here? . . . . .	47
38	■ computational hardness assumptions . . . . .	48
39	■ check reference . . . . .	48
40	■ check reference . . . . .	48
41	■ explain last sentence more . . . . .	49
42	■ “equation”? . . . . .	50
43	■ check reference . . . . .	50
44	■ what’s the difference between $\mathbb{F}_p^*$ and $\mathbb{Z}_p^*$ ? . . . . .	50
45	■ Legendre symbol . . . . .	50
46	■ Euler’s formular . . . . .	50
47	■ These are only explained later in the text, ‘4.33’ . . . . .	50
48	■ are these going to be relevant later? yes, they are used in various snark proof systems	51
49	■ TODO: theorem: every factor of order defines a subgroup... . . . . .	51
50	■ Is there a term for this property? . . . . .	51

















































51	■ a few examples? . . . . .	53
52	■ check reference . . . . .	54
53	■ TODO: DOUBLE CHECK THIS REASONING. . . . .	54
54	■ Mirco: We can do better than this . . . . .	56
55	■ check reference . . . . .	57
56	■ add reference . . . . .	58
57	■ pseudorandom . . . . .	58
58	■ oracle . . . . .	58
59	■ check reference . . . . .	58
60	■ add reference . . . . .	62
61	■ Abelian groups . . . . .	62
62	■ codomain . . . . .	62
63	■ Check change of wording . . . . .	62
64	■ Expand on this? . . . . .	63
65	■ check reference . . . . .	63
66	■ S: are we introducing elliptic curves in section 1 or 2? . . . . .	65
67	■ check reference . . . . .	65
68	■ check reference . . . . .	65
69	■ add reference . . . . .	65
70	■ check reference . . . . .	66
71	■ write paragraph on exponentiation . . . . .	66
72	■ add reference . . . . .	66
73	■ check reference . . . . .	66
74	■ add reference . . . . .	66
75	■ group pairings . . . . .	66
76	■ add reference . . . . .	68
77	■ check reference . . . . .	68
78	■ check reference . . . . .	70
79	■ add reference . . . . .	71
80	■ TODO: Elliptic Curve asymmetric cryptography examples. Private key, generator,	
81	public key. . . . .	73
82	■ add reference . . . . .	73
83	■ maybe remove this sentence? . . . . .	73
84	■ affine space . . . . .	73
85	■ cusps . . . . .	74
86	■ self-intersections . . . . .	74
87	■ check reference . . . . .	75
88	■ check reference . . . . .	76
89	■ jubjub . . . . .	76
90	■ check reference . . . . .	76
91	■ affine plane . . . . .	76
92	■ check reference . . . . .	77
93	■ check reference . . . . .	77
94	■ check reference . . . . .	78
95	■ sign . . . . .	78
96	■ more explanation of what the sign is . . . . .	78
97	■ check reference . . . . .	78
98	■ S: I don't follow this at all . . . . .	79

99	check reference	79
100	add explanation of how this shows what we claim	79
101	should this def. be moved even earlier?	80
102	chord line	80
103	tangential	80
104	tangent line	80
105	remove $Q$ ?	80
106	where?	81
107	check reference	81
108	check reference	81
109	check reference	81
110	check reference	82
111	check reference	82
112	check reference	83
113	check reference	83
114	check reference	84
115	add term	84
116	add term	84
117	add reference	84
118	cofactor clearing	84
119	add reference	84
120	check reference	84
121	check reference	85
122	add reference	85
123	add reference	85
124	check reference	85
125	check reference	85
126	check reference	86
127	check reference	86
128	check reference	86
129	Explain how	86
130	write example	87
131	check reference	87
132	add reference	87
133	check reference	87
134	add reference	88
135	check reference	88
136	add reference	88
137	check reference	88
138	add reference	88
139	check reference	88
140	add reference	88
141	add reference	88
142	add reference	88
143	check reference	88
144	check reference	88
145	Check if following Alg is floated too far	89
146	add reference	89

---

147	 add reference . . . . .	89
148	 write up this part . . . . .	89
149	 is the label in L <sup>A</sup> T <sub>E</sub> X correct here? . . . . .	91
150	 check reference . . . . .	91
151	 check reference . . . . .	91
152	 check reference . . . . .	91
153	 check reference . . . . .	92
154	 check reference . . . . .	92
155	 check reference . . . . .	93
156	 check reference . . . . .	93
157	 check reference . . . . .	93
158	 check reference . . . . .	93
159	 check reference . . . . .	93
160	 add reference . . . . .	93
161	 check reference . . . . .	95
162	 check reference . . . . .	95
163	 check reference . . . . .	95
164	 check reference . . . . .	95
165	 check reference . . . . .	95
166	 check reference . . . . .	97
167	 check reference . . . . .	97
168	 check reference . . . . .	98
169	 either expand on this or delete it . . . . .	98
170	 add reference . . . . .	98
171	 check reference . . . . .	98
172	 check reference . . . . .	98
173	 check reference . . . . .	98
174	 check reference . . . . .	98
175	 check reference . . . . .	98
176	 check reference . . . . .	99
177	 check reference . . . . .	99
178	 check reference . . . . .	100
179	 check reference . . . . .	100
180	 add reference . . . . .	100
181	 add reference . . . . .	100
182	 This needs to be written (in Algebra) . . . . .	100
183	 add reference . . . . .	100
184	 add reference . . . . .	100
185	 check reference . . . . .	100
186	 towers of curve extensions . . . . .	101
187	 check reference . . . . .	101
188	 check reference . . . . .	101
189	 check reference . . . . .	101
190	 check reference . . . . .	102
191	 add reference . . . . .	102
192	 check reference . . . . .	103
193	 S: either add more explanation or move to a footnote . . . . .	103
194	 type 3 pairing-based cryptography . . . . .	103

---

195	 add references? . . . . .	103
196	 check reference . . . . .	104
197	 check reference . . . . .	104
198	 check floating of algorithm . . . . .	105
199	 add references . . . . .	105
200	 check reference . . . . .	106
201	 add reference . . . . .	106
202	 check reference . . . . .	106
203	 check reference . . . . .	106
204	 add reference . . . . .	107
205	 should all lines of all algorithms be numbered? . . . . .	107
206	 check reference . . . . .	108
207	 check reference . . . . .	108
208	 check reference . . . . .	108
209	 check if the algorithm is floated properly . . . . .	108
210	 check reference . . . . .	108
211	 again? . . . . .	110
212	 check reference . . . . .	110
213	 circuit . . . . .	110
214	 signature schemes . . . . .	110
215	 add reference . . . . .	110
216	 check reference . . . . .	111
217	 check reference . . . . .	111
218	 add references . . . . .	111
219	 add reference . . . . .	111
220	 reference text to be written in Algebra . . . . .	111
221	 check reference . . . . .	111
222	 check reference . . . . .	111
223	 check reference . . . . .	112
224	 add reference . . . . .	112
225	 algebraic closures . . . . .	112
226	 check reference . . . . .	112
227	 check reference . . . . .	113
228	 check reference . . . . .	113
229	 check reference . . . . .	113
230	 check reference . . . . .	114
231	 disambiguate . . . . .	114
232	 add reference . . . . .	114
233	 unify terminology . . . . .	114
234	 check reference . . . . .	115
235	 actually make this a table? . . . . .	115
236	 exercise still to be written? . . . . .	116
237	 add reference . . . . .	116
238	 check reference . . . . .	116
239	 check reference . . . . .	116
240	 add reference . . . . .	117
241	 check reference . . . . .	118
242	 check reference . . . . .	118

243	check reference . . . . .	118
244	add reference . . . . .	119
245	check reference . . . . .	119
246	check reference . . . . .	119
247	check reference . . . . .	120
248	what does this mean? Maybe just delete it . . . . .	121
249	write up this part . . . . .	122
250	add reference . . . . .	122
251	check reference . . . . .	122
252	cyclotomic polynomial . . . . .	122
253	Pholaard-rho attack . . . . .	122
254	todo . . . . .	122
255	why? Because in this book elliptic curves are only defined for fields of chracteristic $> 3$	123
256	check reference . . . . .	123
257	check reference . . . . .	123
258	what does this mean? . . . . .	123
259	add reference . . . . .	123
260	add reference . . . . .	123
261	check reference . . . . .	123
262	check reference . . . . .	124
263	add reference . . . . .	125
264	add exercise . . . . .	125
265	check reference . . . . .	126
266	add reference . . . . .	126
267	add reference . . . . .	126
268	add reference . . . . .	126
269	check reference . . . . .	127
270	check reference . . . . .	127
271	add reference . . . . .	127
272	add reference . . . . .	127
273	add reference . . . . .	128
274	check reference . . . . .	128
275	add reference . . . . .	128
276	add reference . . . . .	128
277	finish writing this up . . . . .	129
278	add reference . . . . .	129
279	correct computations . . . . .	129
280	fill in missing parts . . . . .	129
281	add reference . . . . .	130
282	check equation . . . . .	130
283	Chapter 1? . . . . .	131
284	"rigorous"? . . . . .	131
285	"proving"? . . . . .	131
286	Add example . . . . .	132
287	M: 1:1 correspondence might actually be wrong . . . . .	132
288	binary tuples . . . . .	132
289	add reference . . . . .	133
290	add reference . . . . .	133

291	check reference	133
292	check reference	133
293	Are we using $w$ and $x$ interchangeably or is there a difference between them?	134
294	check reference	134
295	jubjub	134
296	check reference	134
297	check reference	134
298	check wording	134
299	check reference	134
300	check references	135
301	add reference	135
302	add reference	135
303	check reference	136
304	add reference	136
305	check reference	137
306	check reference	137
307	add reference	137
308	add reference	138
309	Schur/Hadamard product	139
310	add reference	139
311	check reference	139
312	check reference	140
313	add reference	141
314	check reference	142
315	check reference	142
316	check reference	142
317	check reference	142
318	check reference	142
319	add reference	143
320	add reference	144
321	check reference	144
322	check reference	144
323	check reference	145
324	check reference	145
325	add reference	146
326	check reference	148
327	add reference	148
328	check reference	149
329	check reference	149
330	check reference	149
331	Should we refer to R1CS satisfiability (p. 142 here?	150
332	check reference	151
333	add reference	151
334	check reference	151
335	check reference	152
336	check reference	152
337	check reference	153
338	check reference	155































---

339	add reference . . . . .	156
340	"by"? . . . . .	156
341	check reference . . . . .	156
342	check reference . . . . .	156
343	add reference . . . . .	156
344	add reference . . . . .	156
345	check reference . . . . .	156
346	add reference . . . . .	156
347	clarify language . . . . .	158
348	check reference . . . . .	159
349	add reference . . . . .	159
350	check reference . . . . .	159
351	add reference . . . . .	159
352	check references . . . . .	162
353	add references to these languages? . . . . .	162
354	check reference . . . . .	165
355	check reference . . . . .	166
356	check reference . . . . .	166
357	check reference . . . . .	167
358	check reference . . . . .	168
359	check reference . . . . .	168
360	check reference . . . . .	170
361	check reference . . . . .	170
362	check reference . . . . .	171
363	add reference . . . . .	171
364	check reference . . . . .	171
365	add reference . . . . .	171
366	add reference . . . . .	171
367	check reference . . . . .	172
368	check reference . . . . .	172
369	check reference . . . . .	172
370	check reference . . . . .	172
371	add reference . . . . .	172
372	check reference . . . . .	173
373	check reference . . . . .	174
374	"constraints" or "constrained"? . . . . .	174
375	check reference . . . . .	175
376	"constraints" or "constrained"? . . . . .	175
377	add reference . . . . .	175
378	"constraints" or "constrained"? . . . . .	175
379	add reference . . . . .	176
380	check references . . . . .	176
381	check reference . . . . .	176
382	add reference . . . . .	177
383	can we rotate this by 90°? . . . . .	177
384	check reference . . . . .	178
385	add reference . . . . .	178
386	add reference . . . . .	178

387	shift . . . . .	180
388	bishift . . . . .	181
389	add reference . . . . .	182
390	check reference . . . . .	183
391	Add example . . . . .	184
392	add reference . . . . .	185
393	add reference . . . . .	186
394	check reference . . . . .	187
395	add reference . . . . .	187
396	add reference . . . . .	187
397	check reference . . . . .	188
398	add reference . . . . .	188
399	add reference . . . . .	188
400	add reference . . . . .	190
401	check reference . . . . .	191
402	check reference . . . . .	192
403	common reference string . . . . .	192
404	simulation trapdoor . . . . .	192
405	check reference . . . . .	192
406	check reference . . . . .	192
407	add reference . . . . .	193
408	check reference . . . . .	193
409	check reference . . . . .	193
410	check reference . . . . .	193
411	"invariable"? . . . . .	193
412	explain why . . . . .	194
413	4 examples have the same title. Change it to be distinct . . . . .	194
414	check reference . . . . .	194
415	add reference . . . . .	194
416	check reference . . . . .	194
417	add reference . . . . .	194
418	add reference . . . . .	195
419	add reference . . . . .	196
420	check reference . . . . .	197
421	add reference . . . . .	197
422	add reference . . . . .	198
423	check reference . . . . .	198
424	check reference . . . . .	198
425	add reference . . . . .	198
426	add reference . . . . .	198
427	check reference . . . . .	199
428	add reference . . . . .	199
429	add reference . . . . .	199
430	add reference . . . . .	199
431	check reference . . . . .	199
432	add reference . . . . .	199
433	add reference . . . . .	199
434	add reference . . . . .	199

---

435		add reference . . . . .	199
436		add reference . . . . .	200
437		add reference . . . . .	200
438		add reference . . . . .	200
439		add reference . . . . .	200
440		check reference . . . . .	202
441		check reference . . . . .	202
442		add reference . . . . .	202
443		add reference . . . . .	202
444		add reference . . . . .	202
445		add reference . . . . .	202
446		add reference . . . . .	203
447		add reference . . . . .	203
448		add reference . . . . .	203
449		add reference . . . . .	203
450		fix error . . . . .	203
451		add reference . . . . .	203
452		check reference . . . . .	204
453		add reference . . . . .	204
454		add reference . . . . .	204
455		add reference . . . . .	204
456		add reference . . . . .	205
457		add reference . . . . .	205
458		add reference . . . . .	205
459		add reference . . . . .	205
460		add reference . . . . .	205
461		add reference . . . . .	205
462		add reference . . . . .	205
463		add reference . . . . .	206

464

# MoonMath manual

465

TechnoBob and the Least Scruples crew

466

June 23, 2022

# Contents

468	<b>1 Introduction</b>	<b>5</b>
469	1.1 Target audience . . . . .	5
470	1.2 The Zoo of Zero-Knowledge Proofs . . . . .	6
471	To Do List . . . . .	8
472	Points to cover while writing . . . . .	8
473	<b>2 Preliminaries</b>	<b>9</b>
474	2.1 Preface and Acknowledgements . . . . .	9
475	2.2 Purpose of the book . . . . .	9
476	2.3 How to read this book . . . . .	10
477	2.4 Cryptological Systems . . . . .	10
478	2.5 SNARKS . . . . .	10
479	2.6 complexity theory . . . . .	10
480	2.6.1 Runtime complexity . . . . .	10
481	2.7 Software Used in This Book . . . . .	11
482	2.7.1 Sagemath . . . . .	11
483	<b>3 arithmetic</b>	<b>12</b>
484	3.1 Introduction . . . . .	12
485	3.1.1 Aims and target audience . . . . .	12
486	3.1.2 The structure of this chapter . . . . .	13
487	3.2 Integer arithmetic . . . . .	13
488	Euclidean Division . . . . .	16
489	The Extended Euclidean Algorithm . . . . .	18
490	Coprime Integers . . . . .	20
491	3.3 Modular arithmetic . . . . .	20
492	Congruence . . . . .	20
493	Computational Rules . . . . .	21
494	The Chinese Remainder Theorem . . . . .	23
495	Remainder Class Representation . . . . .	25
496	Modular Inverses . . . . .	26
497	3.4 Polynomial arithmetic . . . . .	30
498	Polynomial arithmetic . . . . .	33
499	Euklidean Division . . . . .	35
500	Prime Factors . . . . .	37
501	Lagrange interpolation . . . . .	38

502	<b>4 Algebra</b>	<b>41</b>
503	4.1 Commutative Groups . . . . .	41
504	Finite groups . . . . .	43
505	Generators . . . . .	43
506	The exponential map . . . . .	44
507	Factor Groups . . . . .	45
508	Pairings . . . . .	46
509	4.1.1 Cryptographic Groups . . . . .	47
510	The discrete logarithm assumption . . . . .	48
511	The decisional Diffie–Hellman assumption . . . . .	49
512	The computational Diffie–Hellman assumption . . . . .	50
513	Cofactor Clearing . . . . .	51
514	4.1.2 Hashing to Groups . . . . .	51
515	Hash functions . . . . .	51
516	Hashing to cyclic groups . . . . .	53
517	Hashing to modular arithmetics . . . . .	54
518	Pedersen Hashes . . . . .	57
519	MimC Hashes . . . . .	58
520	Pseudorandom Functions in DDH-A groups . . . . .	58
521	4.2 Commutative Rings . . . . .	58
522	Hashing to Commutative Rings . . . . .	62
523	4.3 Fields . . . . .	62
524	4.3.1 Prime fields . . . . .	63
525	Square Roots . . . . .	65
526	Exponentiation . . . . .	66
527	Hashing into prime fields . . . . .	66
528	MiMC Hash functions . . . . .	66
529	4.3.2 Extension Fields . . . . .	66
530	Hashing into extension fields . . . . .	70
531	4.4 Projective Planes . . . . .	70
532	<b>5 Elliptic Curves</b>	<b>73</b>
533	5.1 Elliptic Curve Arithmetics . . . . .	73
534	5.1.1 Short Weierstraß Curves . . . . .	73
535	Affine short Weierstraß form . . . . .	74
536	Affine compressed representation . . . . .	78
537	Affine group law . . . . .	79
538	Scalar multiplication . . . . .	84
539	Projective short Weierstraß form . . . . .	87
540	Projective Group law . . . . .	88
541	Coordinate Transformations . . . . .	89
542	5.1.2 Montgomery Curves . . . . .	89
543	Affine Montgomery Form . . . . .	91
544	Affine Montgomery coordinate transformation . . . . .	92
545	Montgomery group law . . . . .	94
546	5.1.3 Twisted Edwards Curves . . . . .	95
547	Twisted Edwards Form . . . . .	95
548	Twisted Edwards group law . . . . .	97

549	5.2	Elliptic Curve Pairings . . . . .	98
550		Embedding Degrees . . . . .	98
551		Elliptic Curves over extension fields . . . . .	99
552		Full torsion groups . . . . .	100
553		Torsion subgroups . . . . .	103
554		The Weil pairing . . . . .	105
555	5.3	Hashing to Curves . . . . .	107
556		Try-and-increment hash functions . . . . .	108
557	5.4	Constructing elliptic curves . . . . .	110
558		The Trace of Frobenius . . . . .	111
559		The $j$ -invariant . . . . .	112
560		The Complex Multiplication Method . . . . .	113
561		The <i>BLS6_6</i> pen-and-paper curve . . . . .	122
562		Hashing to pairing groups . . . . .	129
563	<b>6</b>	<b>Statements</b>	<b>131</b>
564	6.1	Formal Languages . . . . .	131
565		Decision Functions . . . . .	132
566		Instance and Witness . . . . .	135
567		Modularity . . . . .	138
568	6.2	Statement Representations . . . . .	138
569	6.2.1	Rank-1 Quadratic Constraint Systems . . . . .	138
570		R1CS representation . . . . .	139
571		R1CS Satisfiability . . . . .	141
572		Modularity . . . . .	142
573	6.2.2	Algebraic Circuits . . . . .	143
574		Algebraic circuit representation . . . . .	143
575		Circuit Execution . . . . .	148
576		Circuit Satisfiability . . . . .	150
577		Associated Constraint Systems . . . . .	151
578	6.2.3	Quadratic Arithmetic Programs . . . . .	156
579		QAP representation . . . . .	156
580		QAP Satisfiability . . . . .	158
581	<b>7</b>	<b>Circuit Compilers</b>	<b>162</b>
582	7.1	A Pen-and-Paper Language . . . . .	162
583	7.1.1	The Grammar . . . . .	162
584	7.1.2	The Execution Phases . . . . .	164
585		The Setup Phase . . . . .	164
586		The Prover Phase . . . . .	166
587	7.2	Common Programing concepts . . . . .	166
588	7.2.1	Primitive Types . . . . .	166
589		The base-field type . . . . .	167
590		The Subtraction Constraint System . . . . .	170
591		The Inversion Constraint System . . . . .	171
592		The Division Constraint System . . . . .	172
593		The boolean Type . . . . .	173
594		The boolean Constraint System . . . . .	173

595		The AND operator constraint system . . . . .	174
596		The OR operator constraint system . . . . .	174
597		The NOT operator constraint system . . . . .	175
598		Modularity . . . . .	176
599		Arrays . . . . .	179
600		The Unsigned Integer Type . . . . .	179
601		The uN Constraint System . . . . .	180
602		The Unsigned Integer Operators . . . . .	181
603	7.2.2	Control Flow . . . . .	182
604		The Conditional Assignment . . . . .	182
605		Loops . . . . .	184
606	7.2.3	Binary Field Representations . . . . .	185
607	7.2.4	Cryptographic Primitives . . . . .	187
608		Twisted Edwards curves . . . . .	187
609		Twisted Edwards curve constraints . . . . .	187
610		Twisted Edwards curve addition . . . . .	188
611	<b>8</b>	<b>Zero Knowledge Protocols</b>	<b>190</b>
612	8.1	Proof Systems . . . . .	190
613	8.2	The “Groth16” Protocol . . . . .	191
614		The Setup Phase . . . . .	193
615		The Prover Phase . . . . .	198
616		The Verification Phase . . . . .	201
617		Proof Simulation . . . . .	203
618	<b>9</b>	<b>Exercises and Solutions</b>	<b>207</b>



# Chapter 1

## Introduction

This is dump from other papers as inspiration for the intro:

Zero knowledge proofs are a class of cryptographic protocols in which one can prove honest computation without revealing the inputs to that computation. A simple high-level example of a zero-knowledge proof is the ability to prove one is of legal voting age without revealing the respective age. In a typical zero knowledge proof system, there are two participants: a prover and a verifier. A prover will present a mathematical proof of computation to a verifier to prove honest computation. The verifier will then confirm whether the prover has performed honest computation based on predefined methods. Zero knowledge proofs are of particular interest to public blockchain activities as the verifier can be codified in smart contracts as opposed to trusted parties or third-party intermediaries.

Zero-knowledge proofs (ZKPs) are an important privacy-enhancing tool from cryptography. They allow proving the veracity of a statement, related to confidential data, without revealing any information beyond the validity of the statement. ZKPs were initially developed by the academic community in the 1980s, and have seen tremendous improvements since then. They are now of practical feasibility in multiple domains of interest to the industry, and to a large community of developers and researchers. ZKPs can have a positive impact in industries, agencies, and for personal use, by allowing privacy-preserving applications where designated private data can be made useful to third parties, despite not being disclosed to them.

ZKP systems involve at least two parties: a prover and a verifier. The goal of the prover is to convince the verifier that a statement is true, without revealing any additional information. For example, suppose the prover holds a birth certificate digitally signed by an authority. In order to access some service, the prover may have to prove being at least 18 years old, that is, that there exists a birth certificate, tied to the identity of the prover and digitally signed by a trusted certification authority, stating a birthdate consistent with the age claim. A ZKP allows this, without the prover having to reveal the birthdate.

### 1.1 Target audience

This book is accessible for both beginners and experienced developers alike. Concepts are gradually introduced in a logical and steady pace. Nonetheless, the chapters lend themselves rather well to being read in a different order. More experienced developers might get the most benefit by jumping to the chapters that interest them most. If you like to learn by example, then you should go straight to the chapter on Using Clarity.

It is assumed that you have a basic understanding of programming and the underlying logical concepts. The first chapter covers the general syntax of Clarity but it does not delve into what

programming itself is all about. If this is what you are looking for, then you might have a more difficult time working through this book unless you have an (undiscovered) natural affinity for such topics. Do not let that dissuade you though, find an introductory programming book and press on! The straightforward design of Clarity makes it a great first language to pick up.

## 1.2 The Zoo of Zero-Knowledge Proofs

First, a list of zero-knowledge proof systems:

1. Pinocchio (2013): Paper

– Notes: trusted setup

2. BCGTV (2013): Paper

– Notes: trusted setup, implementation

3. BCTV (2013): Paper

– Notes: trusted setup, implementation

4. Groth16 (2016): Paper

– Notes: trusted setup

– Other resources: Talk in 2019 by Georgios Konstantopoulos

5. GM17 (2017): Paper

– Notes: trusted setup

– Other resources: later Simulation extractability in ROM, 2018

6. Bulletproofs (2017): Paper

– Notes: no trusted setup

– Other resources: Polynomial Commitment Scheme on DL, 2016 and KZG10, Polynomial Commitment Scheme on Pairings, 2010

7. Ligero (2017): Paper

– Notes: no trusted setup

– Other resources:

8. Hyrax (2017): Paper

– Notes: no trusted setup

– Other resources:

9. STARKs (2018): Paper

– Notes: no trusted setup

– Other resources:

## 10. Aurora (2018): Paper

- Notes: transparent SNARK

- Other resources:

## 11. Sonic (2019): Paper

- Notes: SNORK - SNARK with universal and updateable trusted setup, PCS-based

- Other resources: Blog post by Mary Maller from 2019 and work on updateable and universal setup from 2018

## 12. Libra (2019): Paper

- Notes: trusted setup

- Other resources:

## 13. Spartan (2019): Paper

- Notes: transparent SNARK

- Other resources:

## 14. PLONK (2019): Paper

- Notes: SNORK, PCS-based

- Other resources: Discussion on Plonk systems and Awesome Plonk list

## 15. Halo (2019): Paper

- Notes: no trusted setup, PCS-based, recursive

- Other resources:

## 16. Marlin (2019): Paper

- Notes: SNORK, PCS-based

- Other resources: Rust Github

## 17. Fractal (2019): Paper

- Notes: Recursive, transparent SNARK

- Other resources:

## 18. SuperSonic (2019): Paper

- Notes: transparent SNARK, PCS-based

- Other resources: Attack on DARK compiler in 2021

## 19. Redshift (2019): Paper

- Notes: SNORK, PCS-based

- Other resources:

**Other resources on the zoo:** Awesome ZKP list on Github, ZKP community with the reference document

**To Do List**

- Make table for prover time, verifier time, and proof size
- Think of categories - *Achieved Goals*: Trusted setup or not, Post-quantum or not, ...
- Think of categories - *Mathematical background*: Polynomial commitment scheme, ...
- ... while we discuss the points above, we should also discuss a common notation/language for all these things. (E.g. transparent SNARK/no trusted setup/STARK)

**Points to cover while writing**

- Make a historical overview over the "discovery" of the different ZKP systems
- Make reader understand what paper is build on what result etc. - the tree of publications!
- Make reader understand the different terminology, e.g. SNARK/SNORK/STARK, PCS, R1CS, updateable, universal, ...
- Make reader understand the mathematical assumptions - and what this means for the zoo.
- Where will the development/evolution go? What are bottlenecks?

**Other topics I fell into while compiling this list**

- Vector commitments: <https://eprint.iacr.org/2020/527.pdf>
- Snark1: <http://ace.cs.ohio.edu/~gstewart/papers/snaark1.pdf>
- Virgo?: [https://people.eecs.berkeley.edu/~kubitron/courses/cs262a-F19/projects/reports/project5\\_report\\_ver2.pdf](https://people.eecs.berkeley.edu/~kubitron/courses/cs262a-F19/projects/reports/project5_report_ver2.pdf)

## Chapter 2

## Preliminaries

### 2.1 Preface and Acknowledgements

This book began as a set of lecture and notes accompanying the zk-Summit 0x and 0xx .... It arose from the desire to collect the scattered information of snarks [] and present them to an audience that does not have a strong background in cryptography []

### 2.2 Purpose of the book

The first version of this book is written by security auditors at Least Authority where we audited quite a few snark based systems. Its included "what we have learned" destilate of the time we spend on various audits.

We intend to let illustrative examples drive the discussion and present the key concepts of pairing computation with as little machinery as possible. For those that are fresh to pairing-based cryptography, it is our hope that this chapter might be particularly useful as a first read and prelude to more complete or advanced expositions (e.g. the related chapters in [Gal12]).

On the other hand, we also hope our beginner-friendly intentions do not leave any sophisticated readers dissatisfied by a lack of formality or generality, so in cases where our discussion does sacrifice completeness, we will at least endeavour to point to where a more thorough exposition can be found.

One advantage of writing a survey on pairing computation in 2012 is that, after more than a decade of intense and fast-paced research by mathematicians and cryptographers around the globe, the field is now racing towards full maturity. Therefore, an understanding of this text will equip the reader with most of what they need to know in order to tackle any of the vast literature in this remarkable field, at least for a while yet.

Since we are aiming the discussion at active readers, we have matched every example with a corresponding snippet of (hyperlinked) Magma [BCP97] code 1 , where we take inspiration from the helpful Magma pairing tutorial by Dominguez Perez et al. [DKS09].

Early in the book we will develop examples that we then later extend with most of the things we learn in each chapter. This way we incrementally build a few real world snarks but over full fledged cryptographic systems that are nevertheless simple enough to be computed by pen and paper to illustrate all steps in great detail.

## 2.3 How to read this book

Books and papers to read: XXXXXXXXXXXXX

Software to try: XXXXXXXXXXXXXXXXXXXXX

Correctly prescribing the best reading route for a beginner naturally requires individual diagnosis that depends on their prior knowledge and technical preparation.

## 2.4 Cryptological Systems

The science of information security is referred to as *cryptology*. In the broadest sense, it deals with encryption and decryption processes, with digital signatures, identification protocols, cryptographic hash functions, secrets sharing, electronic voting procedures and electronic money. EXPAND

## 2.5 SNARKS

## 2.6 complexity theory

Before we deal with the mathematics behind zero knowledge proof systems, we must first clarify what is meant by the runtime of an algorithm or the time complexity of an entire mathematical problem. This is particularly important for us when we analyze the various snark systems...

For the reader who is interested in complexity theory, we recommend, or example or , as well as the references contained therein.

### 2.6.1 Runtime complexity

The runtime complexity of an algorithm describes, roughly speaking, the amount of elementary computation steps that this algorithm requires in order to solve a problem, depending on the size of the input data.

Of course, the exact amount of arithmetic operations required depends on many factors such as the implementation, the operating system used, the CPU and many more. However, such accuracy is seldom required and is mostly meaningful to consider only the asymptotic computational effort.

In computer science, the runtime of an algorithm is therefore not specified in individual calculation steps, but instead looks for an upper limit which approximates the runtime as soon as the input quantity becomes very large. This can be done using the so-called *Landau notation* (also called big- $\mathcal{O}$ -notation) A precise definition would, however, go beyond the scope of this work and we therefore refer the reader to .

For us, only a rough understanding of transit times is important in order to be able to talk about the security of cryptographic systems. For example,  $\mathcal{O}(n)$  means that the running time of the algorithm to be considered is linearly dependent on the size of the input set  $n$ ,  $\mathcal{O}(n^k)$  means that the running time is polynomial and  $\mathcal{O}(2^n)$  stands for an exponential running time (chapter 2.4).

An algorithm which has a running time that is greater than a polynomial is often simply referred to as *slow*.

A generalization of the runtime complexity of an algorithm is the so-called *time complexity of a mathematical problem*, which is defined as the runtime of the fastest possible algorithm that can still solve this problem ( chapter 3.1).

Since the time complexity of a mathematical problem is concerned with the runtime analysis of all possible (and thus possibly still undiscovered) algorithms, this is often a very difficult and deep-seated question .

For us, the time complexity of the so-called discrete logarithm problem will be important. This is a problem for which we only know slow algorithms on classical computers at the moment, but for which at the same time we cannot rule out that faster algorithms also exist.

STUFF ON CRYPTOGRAPHIC HASH FUNCTIOND

## 2.7 Software Used in This Book

### 2.7.1 Sagemath

It order to provide an interactive learning experience, and to allow getting hands-on with the concepts described in this book, we give examples for how to program them in the Sage programming language. Sage is a dialect of the learning-friendly programming language Python, which was extended and optimized for computing with, in and over algebraic objects. Therefore, we recommend installing Sage before diving into the following chapters.

The installation steps for various system configurations are described on the sage websit <sup>1</sup>. Note however that we use Sage version 9, so if you are using Linux and your package manager only contains version 8, you may need to choose a different installation path, such as using prebuilt binaries.

We recommend the interested reader, who is not familiar with sagemath to read on the many tutorial before starting this book. For example

---

<sup>1</sup><https://doc.sagemath.org/html/en/installation/index.html>

# Chapter 3

## arithmetic

### 3.1 Introduction

#### 3.1.1 Aims and target audience

Sylvia: This subsection should be in the introduction of the book as it applies to the entire math part

How much mathematics do you need to understand **zero-knowledge proofs**? The answer, of course, depends on the level of understanding you aim for. It is possible to describe zero-knowledge proofs without using mathematics at all; however, to read a foundational paper like ? and to understand the internals of snark implementations, some knowledge of mathematics is needed to be able to follow the discussion.

The goal of this chapter is therefore to enable a reader who is starting out with nothing more than basic high school algebra to be able to solve simple tasks in the mathematics underlying most zero knowledge proofs without the need of a computer.

Without a solid grounding in mathematics, someone who is interested in learning the concepts of zero-knowledge proofs, but who has never seen or dealt with, say, a prime field 4.3.1, or an elliptic curve 5, may quickly become overwhelmed. This is not so much due to the complexity of the mathematics needed, but rather because of the vast amount of technical jargon, unknown terms, and obscure symbols that quickly makes a text unreadable, even though the concepts themselves are not actually that complicated. As a result, the reader might either lose interest, or pick up some incoherent bits and pieces of knowledge that, in the worst case scenario, result in immature and unsecure code.

This is why we dedicated this chapter to explaining the mathematical foundations needed to understand the basic concepts underlying snark development. We encourage the reader who is not familiar with basic number theory and elliptic curves to take the time and read this and the following chapters, until they are able to solve at least a few exercises in each chapter.

If, on the other hand, you are already skilled in elliptic curve cryptography, feel free to skip this chapter and only come back to it for reference and comparison. Maybe the most interesting parts are XXX .

We start our explanations at a very basic level, and only assume pre-existing knowledge of fundamental concepts like high school integer arithmetic. At the same time, we'll attempt to teach you to "think mathematically", and to show you that there are numbers and mathematical structures out there that appear to be very different from the things you learned about in high school, but on a deeper level, they are actually quite similar, as we will see in various examples below in this chapter.

Sylvia:  
This subsection should be in the introduction of the book as it applies to the entire math part

zero-knowledge proofs

add references



To make it easier to memorize new concepts and symbols, we might frequently link to definitions in the beginning, but as too many links render a text unreadable, we will assume the reader will become familiar with definitions as the text proceeds at which point we will not link them anymore.

We want to stress, however that this introduction is informal, incomplete and optimized to enable the reader to understand zero-knowledge concepts as efficiently as possible. Our focus and design choices are to include as little theory as necessary, focusing on a wealth of numerical examples. We believe that such an informal, example-driven approach to learning mathematics may make it easier for beginners to digest the material in the initial stages.

For instance, as a beginner, you would probably find it more beneficial to first compute a simple toy **snark** with pen and paper all the way through, before actually developing real-world production-ready systems. In addition, it's useful to have a few simple examples in your head before getting started with reading actual academic papers.

However, in order to be able to derive these toy examples, some mathematical groundwork is needed. This chapter therefore will help the inexperienced reader to focus on what we believe is important, accompanied by exercises that you are encouraged to recompute yourself. Every section usually ends with a list of additional exercises in increasing order of difficulty, to help the reader memorize and apply the concepts.

### 3.1.2 The structure of this chapter

**Sylvia:** This subsection should be in the introduction of the book as it applies to the entire math part

We start with a brief recapitulation of basic integer arithmetic like long division, the greatest common divisor and Euclid's algorithm. After that, we introduce modular arithmetic as **the most important skill** to compute our pen-and-paper examples. We then introduce polynomials, compute their analogs to integer arithmetic and introduce the important concept of Lagrange interpolation.

After this practical warm up, we introduce some basic algebraic terms like groups and fields, because those terms are used very frequently in academic papers relating to zero-knowledge proofs. The beginner is advised to memorize those terms and think about them: Why are they defined the way they are? Can you come up with a better definition? How and why is every rule important and what happens if that rule is dropped?

We define these terms in the general abstract way of mathematics, hoping that the non mathematical trained reader will gradually learn to become comfortable with this style. We then give basic examples and do basic computations with these examples to get familiar with the concepts.

**Sylvia:** This subsection should be in the introduction of the book as it applies to the entire math part

## 3.2 Integer arithmetic

In a sense, integer arithmetic is at the heart of large parts of modern cryptography. Fortunately, most readers will probably remember integer arithmetic from school. It is, however, important that you can confidently apply those concepts to understand and execute computations in the many pen-and-paper examples that form an integral part of the MoonMath Manual. We will therefore recapitulate basic arithmetic concepts to refresh your memory and fill any knowledge gaps.

In what follows, we use many mathematical notations, which we summarized in the following table 3.2:

Symbol	Meaning of Symbol
$=$	equals
$:=$	defining the symbol on the r
$\in$	element from a set
$\Leftrightarrow$	logical equivalence
$\sum_{j=n}^k a_j$	summation

Sylvia: We should put this table into the same introduction as 3.1.1

In this book, we use the symbol  $\mathbb{Z}$  as a short description for the set of all **integers**, that is we write:

$$\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} \quad (3.1)$$

Integers are also known as **whole numbers**, that is, numbers that can be written without fractional parts. Examples of numbers that are **not** integers are  $\frac{2}{3}$ , 1.2 and  $-1280.006$ .

If  $a \in \mathbb{Z}$  is an integer, then we write  $|a|$  for the **absolute value** of  $a$ , that is, the non-negative value of  $a$  without regard to its sign:

$$|4| = 4 \quad (3.2)$$

$$|-4| = 4 \quad (3.3)$$

We use the symbol  $\mathbb{N}$  for the set of all positive integers, usually called the set of **natural numbers** and  $\mathbb{N}_0$  for the set of all non negative integers. So whenever you see the symbol  $\mathbb{N}$ , think of the set of all positive integers excluding the number 0:

$$\mathbb{N} := \{1, 2, 3, \dots\} \quad \mathbb{N}_0 := \{0, 1, 2, 3, \dots\}$$

In addition, we use the symbol  $\mathbb{Q}$  for the set of all **rational numbers**, which can be represented as the set of all fractions  $\frac{n}{m}$ , where  $n \in \mathbb{Z}$  is an integer and  $m \in \mathbb{N}$  is a natural number, such that there is no other fraction  $\frac{n'}{m'}$  and natural number  $k \in \mathbb{N}$  with  $k \neq 1$  and

$$\frac{n}{m} = \frac{k \cdot n'}{k \cdot m'} \quad (3.4)$$

The sets  $\mathbb{N}$ ,  $\mathbb{Z}$  and  $\mathbb{Q}$  have a notion of addition and multiplication defined on them. Most of us are probably able to do many integer computations in our head, but this gets more and more difficult as these increase in complexity. We will frequently invoke the SageMath system (2.7.1) for more complicated computations (We define rings and fields later in this book):

```
sage: ZZ # A sage notation for the integers
Integer Ring
sage: NN # A sage notation for the natural numbers
Non negative integer semiring
sage: QQ # A sage notation for the rational numbers
Rational Field
sage: ZZ(5) # Get an element from the integers
5
```

Sylvia:  
We should  
put this  
table into  
the same  
introduc-  
tion as  
3.1.1

@jan  
@anna  
double  
check this  
definition.  
Is it clear  
enough?  
Proper  
definition  
requires  
the con-  
cept of  
equiv-  
alence or  
coprime-  
ness first

```

928 sage: ZZ(5) + ZZ(3) 9
929 8 10
930 sage: ZZ(5) * NN(3) 11
931 15 12
932 sage: ZZ.random_element(10**50) 13
933 58326321350045030553833939523356241798840389665425 14
934 sage: ZZ(27713).str(2) # Binary string representation 15
935 110110001000001 16
936 sage: NN(27713).str(2) # Binary string representation 17
937 110110001000001 18
938 sage: ZZ(27713).str(16) # Hexadecimal string representation 19
939 6c41 20

```

One set of numbers that is of particular interest to us is the set of **prime numbers**, which are natural numbers  $p \in \mathbb{N}$  with  $p \geq 2$ , which are only divisible by themselves and by 1. All prime numbers apart from the number 2 are called **odd prime numbers**. We write  $\mathbb{P}$  for the set of all prime numbers and  $\mathbb{P}_{\geq 3}$  for the set of all odd prime numbers. The set of prime numbers  $\mathbb{P}$  is an infinite set and can be ordered according to size, which means that for any prime number  $p \in \mathbb{P}$  one can always find another prime number  $p' \in \mathbb{P}$  with  $p < p'$ . It follows that there is no largest prime number. Since prime numbers can be ordered by size, we can write them as follows:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, \dots \quad (3.5)$$

As the **fundamental theorem of arithmetic** tells us, prime numbers are, in a certain sense, the basic building blocks from which all other natural numbers are composed. To see that, let  $n \in \mathbb{N}$  be any natural number with  $n > 1$ . Then there are always prime numbers  $p_1, p_2, \dots, p_k \in \mathbb{P}$ , such that

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k. \quad (3.6)$$

This representation is unique for each natural number (except for the order of the factors) and is called the **prime factorization** of  $n$ .

*Example 1* (Prime Factorization). To see what we mean by prime factorization of a number, let's look at the number  $504 \in \mathbb{N}$ . To get its prime factors, we can successively divide it by all prime numbers in ascending order starting with 2:

$$504 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$$

We can double check our findings invoking Sage, which provides an algorithm to factor natural numbers:

```

955 sage: n = NN(504) 21
956 sage: factor(n) 22
957 2^3 * 3^2 * 7 23

```

The computation from the previous example reveals an important observation: Computing the factorization of an integer is computationally expensive, because we have to divide repeatedly by all prime numbers smaller than the number itself until all factors are prime numbers themselves. From this, an important question arises: How fast can we compute the prime factorization of a natural number? This question is the famous **integer factorization problem** and, as far as we know, there is currently no method known that can factor integers much faster than the naive approach that just divides the given number by all prime numbers in ascending order.

On the other hand computing the product of a given set of prime numbers, is fast (just multiply all factors) and this simple observation implies that the two processes "prime number multiplication" on the one side and its inverse process "natural number factorization" have very different computational costs. The factorization problem is therefore an example of a so-called **one-way function**: An invertible function that is easy to compute in one direction, but hard to compute in the other direction.

It should be pointed out, however, that the American mathematician Peter W. Shor developed an algorithm in ? which can calculate the prime factorization of a natural number in polynomial time on a quantum computer. The consequence of this is that cryptosystems, which are based on the prime factor problem, are unsafe as soon as practically usable quantum computers become available .

*Exercise 1.* What is the absolute value of the integers  $-123$ ,  $27$  and  $0$ ?

*Exercise 2.* Compute the factorization of  $30030$  and double check your results using Sage.

*Exercise 3.* Consider the following equation  $4 \cdot x + 21 = 5$ . Compute the set of all solutions for  $x$  under the following alternative assumptions:

1. The equation is defined over the natural numbers.

2. The equation is defined over the integers.

*Exercise 4.* Consider the following equation  $2x^3 - x^2 - 2x = -1$ . Compute the set of all solutions  $x$  under the following assumptions:

1. The equation is defined over the natural numbers.

2. The equation is defined over the integers.

3. The equation is defined over the rational numbers.

**Euclidean Division** As we know from high school mathematics, integers can be added, subtracted and multiplied and the result is guaranteed to always be an integer again. On the contrary division in the commonly understood sense is not defined for integers, as, for example,  $7$  divided by  $3$  will not be an integer again. However it is always possible to divide any two integers if we consider division with remainder. So for example  $7$  divided by  $3$  is equal to  $2$  with a remainder of  $1$ , since  $7 = 2 \cdot 3 + 1$ .

It is the content of this section to introduce division with remainder for integers which is usually called **Euclidean division**. It is an essential technique underlying many concepts in this book. The precise definition is as follows:

Let  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z}$  be two integers with  $b \neq 0$ . Then there is always another integer  $m \in \mathbb{Z}$  and a natural number  $r \in \mathbb{N}$ , with  $0 \leq r < |b|$  such that

$$a = m \cdot b + r \quad (3.7)$$

This decomposition of  $a$  given  $b$  is called **Euclidean division**, where  $a$  is called the **dividend**,  $b$  is called the **divisor**,  $m$  is called the **quotient** and  $r$  is called the **remainder**. It can be shown that both the quotient and the remainder always exist and are unique, as long as the divisor is different from  $0$ .

Do we even need this quantum computing excursion?

@jan.  
You wrote: a and b are required to be non-zero in the definition

1002 *Notation and Symbols* 1. Suppose that the numbers  $a, b, m$  and  $r$  satisfy equation (3.7). Then  
 1003 we often write

$$a \operatorname{div} b := m, \quad a \bmod b := r \quad (3.8)$$

1004 to describe the quotient and the remainder of the Euclidean division. We also say that an integer  
 1005  $a$  is divisible by another integer  $b$  if  $a \bmod b = 0$  holds. In this case we also write  $b|a$  and call  
 1006 the integer  $a \operatorname{div} b$  the **cofactor** of  $b$  in  $a$ .

1007 So, in a nutshell Euclidean division is a process of dividing one integer by another in a way  
 1008 that produces a quotient and a non-negative remainder, the latter of which is smaller than the  
 1009 absolute value of the divisor.

1010 A special situation occurs whenever the remainder is zero, because in this case the dividend  
 1011 is divisible by the divisor. Our notation  $b|a$  reflects that.

*Example 2.* Applying Euclidean division and our previously defined notation 3.8 to the dividend  
 $-17$  and the divisor  $4$ , we get

$$-17 \operatorname{div} 4 = -5, \quad -17 \bmod 4 = 3$$

1012 because  $-17 = -5 \cdot 4 + 3$  is the Euclidean division of  $-17$  and  $4$  (the remainder is, by definition,  
 1013 a non-negative number). In this case  $4$  does not divide  $-17$ , as the remainder is not zero. The  
 1014 truth value of the expression  $4|-17$  therefore is FALSE. On the other hand, the truth value of  
 1015  $4|12$  is TRUE, since  $4$  divides  $12$ , as  $12 \bmod 4 = 0$ . We can invoke sage to do the computation  
 1016 for us. We get the following:

```
1017 sage: ZZ(-17) // ZZ(4) # Integer quotient
1018 -5
1019 sage: ZZ(-17) % ZZ(4) # remainder
1020 3
1021 sage: ZZ(4).divides(ZZ(-17)) # self divides other
1022 False
1023 sage: ZZ(4).divides(ZZ(12))
1024 True
```

1025 *Remark 1.* In 3.8 we defined the notation of  $a \operatorname{div} b$  and  $a \bmod b$ , in terms of Euclidean division.  
 1026 It should be noted however that many programming languages like Python and Sage, implement  
 1027 both the operator  $(/)$  as well as the operator  $(\%)$  differently. Programmers should be aware of  
 1028 this, as the discrepancy between the mathematical notation and the implementation in program-  
 1029 ming languages might become the source of subtle bugs in implementations of cryptographic  
 1030 primitives.

To give an example consider the the dividend  $-17$  and the divisor  $-4$ . Note that in contrast  
 to the previous example 2, we have a negative divisor. According to our definition we have

$$-17 \operatorname{div} -4 = 5, \quad -17 \bmod -4 = 3$$

1031 because  $-17 = 5 \cdot (-4) + 3$  is the Euclidean division of  $-17$  and  $-4$  (the remainder is, by  
 1032 definition, a non-negative number). However using the operators  $(/)$  and  $(\%)$  in Sage we get

```
1033 sage: ZZ(-17) // ZZ(-4) # Integer quotient
1034 4
1035 sage: ZZ(-17) % ZZ(-4) # remainder
1036 -1
```

24

25 You  
 26 wrote:  
 27 If these  
 28 should  
 29 only sat-  
 30 isfy the  
 31 equation,  
 why use  
 definition  
 symbols  
 $(:=)$  and  
 not equal-  
 ity sym-  
 bols  $(=)$ ?  
 But this  
 is a defi-  
 nition the  
 symbol  $a$   
 $\operatorname{div} b$  IS  
 DEFINED  
 to be the  
 number

32... Is that  
 33 clear?

34

35

```

1037 sage: ZZ(-17).quo_rem(ZZ(-4)) # not Euclidean division 36
1038 (4, -1) 37

```

1039 Methods to compute Euclidean division for integers are called **integer division algorithms**.  
 1040 Probably the best known algorithm is the so-called **long division**, which most of us might have  
 1041 learned in school.

1042 As long division is the standard method used for pen-and-paper division of multi-digit num-  
 1043 bers expressed in decimal notation, the reader should become familiar with it as we use it  
 1044 throughout this book when we do simple pen-and-paper computations. However, instead of  
 1045 defining the algorithm formally, we rather give some examples that will hopefully make the  
 1046 process clear.

1047 In a nutshell, the algorithm loops through the digits of the dividend from the left to right,  
 1048 subtracting the largest possible multiple of the divisor (at the digit level) at each stage; the  
 1049 multiples then become the digits of the quotient, and the remainder is the first digit of the  
 1050 dividend.

1051 *Example 3 (Integer Long Division).* To give an example of integer long division algorithm, lets  
 1052 divide the integer  $a = 143785$  by the number  $b = 17$ . Our goal is therefore to find solutions  
 1053 to equation 3.7, that is, we need to find the quotient  $m \in \mathbb{Z}$  and the remainder  $r \in \mathbb{N}$  such that  
 1054  $143785 = m \cdot 17 + r$ . Using a notation that is mostly used in Commonwealth countries, we  
 1055 compute as follows:

$$\begin{array}{r}
 8457 \\
 17 \overline{) 143785} \\
 \underline{136} \phantom{00} \\
 77 \phantom{00} \\
 \underline{68} \phantom{00} \\
 98 \phantom{00} \\
 \underline{85} \phantom{00} \\
 135 \phantom{00} \\
 \underline{119} \phantom{00} \\
 16
 \end{array}
 \tag{3.9}$$

1056 We therefore get  $m = 8457$  as well as  $r = 16$  and indeed we have  $143785 = 8457 \cdot 17 + 16$ ,  
 1057 which we can double check invoking Sage:

```

1058 sage: ZZ(143785).quo_rem(ZZ(17)) 38
1059 (8457, 16) 39
1060 sage: ZZ(143785) == ZZ(8457)*ZZ(17) + ZZ(16) # check 40
1061 True 41

```

1062 *Exercise 5 (Integer Long Division).* Find an  $m \in \mathbb{Z}$  as well as an  $r \in \mathbb{N}$  with  $0 \leq r < |b|$  such that  
 1063  $a = m \cdot b + r$  holds for the following pairs  $(a, b) = (27, 5)$ ,  $(a, b) = (27, -5)$ ,  $(a, b) = (127, 0)$ ,  
 1064  $(a, b) = (-1687, 11)$  and  $(a, b) = (0, 7)$ . In which cases are your solutions unique?

1065 *Exercise 6 (Long Division Algorithm).* Write an algorithm that computes integer long division  
 1066 and handling all edge cases properly.

1067 **The Extended Euclidean Algorithm** One of the most critical parts in this book is the so  
 1068 called modular arithmetic which we will define in 3.3 and its application in the computations of  
 1069 **prime fields** as defined in 4.3.1. To be able to do computations in modular arithmetic, we have

to get familiar with the so-called **extended Euclidean algorithm**. We therefore introduce this algorithm here.

The **greatest common divisor** (GCD) of two non-zero integers  $a$  and  $b$ , is defined as the greatest non-zero natural number  $d$  such that  $d$  divides both  $a$  and  $b$ , that is,  $d|a$  as well as  $d|b$ . We write  $\gcd(a, b) := d$  for this number. Since the natural number 1 divides any other integer, 1 is always a common divisor of any two non-zero integers. However it must not be the greatest.

A common method to compute the greatest common divisor is the so called Euclidean algorithm. However since we don't need that algorithm in this book, we will introduce the Extended Euclidean algorithm which is a method to calculate the greatest common divisor of two natural numbers  $a$  and  $b \in \mathbb{N}$ , as well as two additional integers  $s, t \in \mathbb{Z}$ , such that the following equation holds:

$$\gcd(a, b) = s \cdot a + t \cdot b \quad (3.10)$$

The pseudocode in algorithm 1 shows in detail how to calculate the greatest common divisor and the numbers  $s$  and  $t$  with the extended Euclidean algorithm:

---

**Algorithm 1** Extended Euclidean Algorithm

---

**Require:**  $a, b \in \mathbb{N}$  with  $a \geq b$

**procedure** EXT-EUCLID( $a, b$ )

$r_0 \leftarrow a$

$r_1 \leftarrow b$

$s_0 \leftarrow 1$

$s_1 \leftarrow 0$

$k \leftarrow 1$

**while**  $r_k \neq 0$  **do**

$q_k \leftarrow r_{k-1} \text{ div } r_k$

$r_{k+1} \leftarrow r_{k-1} - q_k \cdot r_k$

$s_{k+1} \leftarrow s_{k-1} - q_k \cdot s_k$

$k \leftarrow k + 1$

**end while**

**return**  $\gcd(a, b) \leftarrow r_{k-1}$ ,  $s \leftarrow s_{k-1}$  and  $t := (r_{k-1} - s_{k-1} \cdot a) \text{ div } b$

**end procedure**

**Ensure:**  $\gcd(a, b) = s \cdot a + t \cdot b$

---

The algorithm is simple enough to be done effectively in pen-and-paper examples, where it is common to write it as a table where the rows represent the while-loop and the columns represent the values of the the array  $r$ ,  $s$  and  $t$  with index  $k$ . The following example provides a simple execution:

*Example 4.* To illustrate algorithm 1, we apply it to the numbers  $a = 12$  and  $b = 5$ . Since  $12, 5 \in \mathbb{N}$  as well as  $12 \geq 5$  all requirements are met and we compute as follows:

k	$r_k$	$s_k$	$t_k = (r_k - s_k \cdot a) \text{ div } b$
0	12	1	0
1	5	0	1
2	2	1	-2
3	1	-2	5
4	0		

From this we can see that the greatest common divisor of 12 and 5 is  $\gcd(12, 5) = 1$  and that the equation  $1 = (-2) \cdot 12 + 5 \cdot 5$  holds. We can also invoke sage to double check our findings:



```

1092 sage: ZZ(12).xgcd(ZZ(5)) # (gcd(a,b), s, t)
1093 (1, -2, 5)

```

42

43

1094 *Exercise 7* (Extended Euclidean Algorithm). Find integers  $s, t \in \mathbb{Z}$  such that  $\gcd(a, b) = s \cdot a +$   
 1095  $t \cdot b$  holds for the following pairs  $(a, b) = (45, 10)$ ,  $(a, b) = (13, 11)$ ,  $(a, b) = (13, 12)$ . What  
 1096 pairs  $(a, b)$  are coprime?

1097 *Exercise 8* (Towards Prime fields). Let  $n \in \mathbb{N}$  be a natural number and  $p$  a prime number, such  
 1098 that  $n < p$ . What is the greatest common divisor  $\gcd(p, n)$ ?

1099 *Exercise 9*. Find all numbers  $k \in \mathbb{N}$  with  $0 \leq k \leq 100$  such that  $\gcd(100, k) = 5$ .

1100 *Exercise 10*. Show that  $\gcd(n, m) = \gcd(n + m, m)$  for all  $n, m \in \mathbb{N}$ .

1101 **Coprime Integers** Coprime integers are integers that do not have a common prime number  
 1102 as a factor. As we will see in 3.3 those numbers are important for our purposes because in  
 1103 modular arithmetic, computation that involve coprime numbers are substantially different from  
 1104 computations on non-coprime numbers 3.3.

1105 The naive way to decide if two integers are coprime would be to divide both number suces-  
 1106 sively by all prime numbers smaller then those numbers to see if they share a common prime  
 1107 factor. However two integers are coprime if and only if their greatest common divisor is 1 and  
 1108 hence computing the  $\gcd$  is the preferred method.

1109 *Example 5*. Consider example 4 again. As we have seen, the greatest common divisor of 12  
 1110 and 5 is 1. This implies that the integers 12 and 5 are coprime, since they share no divisor other  
 1111 then 1, which is not a prime number.

1112 *Exercise 11*. Consider exercise 7 again. Which pairs  $(a, b)$  from that exercise are coprime?

### 1113 3.3 Modular arithmetic

1114 **Modular arithmetic** is a system of integer arithmetic, where numbers “wrap around” when  
 1115 reaching a certain value, much like calculations on a clock wrap around whenever the value  
 1116 exceeds the number 12. For example, if the clock shows that it is 11 o’clock, then 20 hours  
 1117 later it will be 7 o’clock, not 31 o’clock. The number 31 has no meaning on a normal clock that  
 1118 shows hours.

1119 The number at which the wrap occurs is called the **modulus**. Modular arithmetic general-  
 1120 izes the clock example to arbitrary moduli and studies equations and phenomena that arise in  
 1121 this new kind of arithmetic. It is of central importance for understanding most modern crypto  
 1122 systems, in large parts because modular arithmetic provides the computational infrastrutute for  
 1123 algebraic types that have cryptographically useful examples of one-way functions.

1124 Although modular arithmetic appears very different from ordinary integer arithmetic that  
 1125 we are all familiar with, we encourage the interested reader to work through the example and to  
 1126 discover that, once they get used to the idea that this is a new kind of calculations, it will seem  
 1127 much less daunting.

1128 **Congruence** In what follows, let  $n \in \mathbb{N}$  with  $n \geq 2$  be a fixed natural number that we will  
 1129 call the **modulus** of our modular arithmetic system. With such an  $n$  given, we can then group  
 1130 integers into classes, by saying that two integers are in the same class, whenever their Euclidean  
 1131 division 3.2 by  $n$  will give the same remainder. We then say that two numbers are **congruent**  
 1132 whenever they are in the same class.



*Example 6.* If we choose  $n = 12$  as in our clock example, then the integers  $-7, 5, 17$  and  $29$  are all congruent with respect to  $12$ , since all of them have the remainder  $5$  if we perform Euclidean division on them by  $12$ . In the picture of an analog 12-hour clock, starting at 5 o'clock, when we add 12 hours we are again at 5 o'clock, representing the number  $17$ . On the other hand, when we subtract 12 hours, we are at 5 o'clock again, representing the number  $-7$ .

We can formalize this intuition of what congruence should be into a proper definition utilizing Euclidean division (as explained previously in 3.2): Let  $a, b \in \mathbb{Z}$  be two integers and  $n \in \mathbb{N}$  a natural number, such that  $n \geq 2$ . Then  $a$  and  $b$  are said to be **congruent with respect to the modulus  $n$** , if and only if the following equation holds

$$a \bmod n = b \bmod n \quad (3.11)$$

If, on the other hand, two numbers are not congruent with respect to a given modulus  $n$ , we call them **incongruent** w.r.t.  $n$ .

A **congruence** is then nothing but an equation "up to congruence", which means that the equation only needs to hold if we take the modulus on both sides. In which case we write

$$a \equiv b \pmod{n} \quad (3.12)$$

*Exercise 12.* Which of the following pairs of numbers are congruent with respect to the modulus  $13$ :  $(5, 19)$ ,  $(13, 0)$ ,  $(-4, 9)$ ,  $(0, 0)$ .

*Exercise 13.* Find all integers  $x$ , such that the congruence  $x \equiv 4 \pmod{6}$  is satisfied.

**Computational Rules** Having defined the notion of a congruence as an equation "up to a modulus", a follow up question is if we can manipulate a congruence similar to an equation. Indeed we can almost apply the same substitution rules to a congruency then to an equation, with the main difference being that for some non-zero integer  $k \in \mathbb{Z}$ , the congruence  $a \equiv b \pmod{n}$  is equivalent to the congruence  $k \cdot a \equiv k \cdot b \pmod{n}$  only, if  $k$  and the modulus  $n$  are coprime 3.2. The following list gives a set of useful rules:

Suppose that integers  $a_1, a_2, b_1, b_2, k \in \mathbb{Z}$  are given. Then the following arithmetic rules hold for congruencies:

- $a_1 \equiv b_1 \pmod{n} \Leftrightarrow a_1 + k \equiv b_1 + k \pmod{n}$  (compatibility with translation)
- $a_1 \equiv b_1 \pmod{n} \Rightarrow k \cdot a_1 \equiv k \cdot b_1 \pmod{n}$  (compatibility with scaling)
- $\gcd(k, n) = 1$  and  $k \cdot a_1 \equiv k \cdot b_1 \pmod{n} \Rightarrow a_1 \equiv b_1 \pmod{n}$
- $k \cdot a_1 \equiv k \cdot b_1 \pmod{k \cdot n} \Rightarrow a_1 \equiv b_1 \pmod{n}$
- $a_1 \equiv b_1 \pmod{n}$  and  $a_2 \equiv b_2 \pmod{n} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$  (compatibility with addition)
- $a_1 \equiv b_1 \pmod{n}$  and  $a_2 \equiv b_2 \pmod{n} \Rightarrow a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}$  (compatibility with multiplication)

Other rules, such as compatibility with subtraction, follow from the rules above. For example, compatibility with subtraction follows from compatibility with scaling by  $k = -1$  and compatibility with addition.

Another property of congruencies, not known in the traditional arithmetic of integers is **Fermat's Little Theorem**. In simple words, it states that, in modular arithmetic, every number

1170 raised to the power of a prime number modulus is congruent to the number itself. Or, to be more  
 1171 precise, if  $p \in \mathbb{P}$  is a prime number and  $k \in \mathbb{Z}$  is an integer, then:

$$k^p \equiv k \pmod{p}, \quad (3.13)$$

1172 If  $k$  is coprime to  $p$ , then we can divide both sides of this congruence by  $k$  and rewrite the  
 1173 expression into the equivalent form

$$k^{p-1} \equiv 1 \pmod{p} \quad (3.14)$$

1174 The following sage code computes example effects of Fermat's little theorem and highlights the  
 1175 effects of the exponent  $k$  being coprime and not coprime to  $p$ :

```

1176 sage: ZZ(137).gcd(ZZ(64))                                44
1177 1                                                            45
1178 sage: ZZ(64)^ZZ(137) % ZZ(137) == ZZ(64) % ZZ(137)      46
1179 True                                                         47
1180 sage: ZZ(64)^ZZ(137-1) % ZZ(137) == ZZ(1) % ZZ(137)      48
1181 True                                                         49
1182 sage: ZZ(1918).gcd(ZZ(137))                                50
1183 137                                                         51
1184 sage: ZZ(1918)^ZZ(137) % ZZ(137) == ZZ(1918) % ZZ(137)   52
1185 True                                                         53
1186 sage: ZZ(1918)^ZZ(137-1) % ZZ(137) == ZZ(1) % ZZ(137)   54
1187 False                                                        55

```

1188 Let's compute an example that contains most of the concepts described in this section:

*Example 7.* Assume that we consider the modulus 6 and that our task is to solve the following congruence for  $x \in \mathbb{Z}$

$$7 \cdot (2x + 21) + 11 \equiv x - 102 \pmod{6}$$

As many rules for congruencies are more or less same as for integers, we can proceed in a similar way as we would if we had an equation to solve. Since both sides of a congruence contain ordinary integers, we can rewrite the left side as follows:  $7 \cdot (2x + 21) + 11 = 14x + 147 + 11 = 14x + 158$ . We can therefore rewrite the congruence into the equivalent form

$$14x + 158 \equiv x - 102 \pmod{6}$$

In the next step we want to shift all instances of  $x$  to left and every other term to the right. So we apply the “compatibility with translation” rules two times. In a first step we choose  $k = -x$  and in a second step we choose  $k = -158$ . Since “compatibility with translation” transforms a congruence into an equivalent form, the solution set will not change and we get

$$\begin{aligned}
 14x + 158 &\equiv x - 102 \pmod{6} \Leftrightarrow \\
 14x - x + 158 - 158 &\equiv x - x - 102 - 158 \pmod{6} \Leftrightarrow \\
 13x &\equiv -260 \pmod{6}
 \end{aligned}$$

If our congruence would just be a normal integer equation, we would divide both sides by 13 to get  $x = -20$  as our solution. However, in case of a congruence, we need to make sure that the modulus and the number we want to divide by are coprime first – only then will we get an equivalent expression (See rule XXX). So we need to find the greatest common divisor

$\gcd(13, 6)$ . Since 13 is prime and 6 is not a multiple of 13, we know that  $\gcd(13, 6) = 1$ , so these numbers are indeed coprime. We therefore compute

$$13x \equiv -260 \pmod{6} \Leftrightarrow x \equiv -20 \pmod{6}$$

Our task is now to find all integers  $x$ , such that  $x$  is congruent to  $-20$  with respect to the modulus 6. So we have to find all  $x$  such

$$x \bmod 6 = -20 \bmod 6$$

Since  $-4 \cdot 6 + 4 = -20$  we know  $-20 \bmod 6 = 4$  and hence we know that  $x = 4$  is a solution to this congruence. However, 22 is another solution since  $22 \bmod 6 = 4$  as well, and so is  $-20$ . In fact, there are infinitely many solutions given by the set

$$\{\dots, -8, -2, 4, 10, 16, \dots\} = \{4 + k \cdot 6 \mid k \in \mathbb{Z}\}$$

Putting all this together, we have shown that the every  $x$  from the set  $\{x = 4 + k \cdot 6 \mid k \in \mathbb{Z}\}$  is a solution to the congruence  $7 \cdot (2x + 21) + 11 \equiv x - 102 \pmod{6}$ . We double ckeck for, say,  $x = 4$  as well as  $x = 4 + 12 \cdot 6 = 76$  using sage:

```

1192 sage: (ZZ(7) * (ZZ(2) * ZZ(4) + ZZ(21)) + ZZ(11)) % ZZ(6) == (ZZ 56
1193       (4) - ZZ(102)) % ZZ(6)
1194 True
1195 sage: (ZZ(7) * (ZZ(2) * ZZ(76) + ZZ(21)) + ZZ(11)) % ZZ(6) == ( 58
1196       ZZ(76) - ZZ(102)) % ZZ(6)
1197 True

```

Readers who had not been familiar with modular arithmetic until now and who might be discouraged by how complicated modular arithmetic seems at this point, should keep two things in mind. First, computing congruencies in modular arithmetic is not really more complicated than computations in more familiar number systems (e.g. rational numbers), it is just a matter of getting used to it. Second, once we introduce the idea of remainder class representations 3.3, computations become conceptually cleaner and more easy to handle.

*Exercise 14.* Consider the modulus 13 and find all solutions  $x \in \mathbb{Z}$  to the following congruence  $5x + 4 \equiv 28 + 2x \pmod{13}$

*Exercise 15.* Consider the modulus 23 and find all solutions  $x \in \mathbb{Z}$  to the following congruence  $69x \equiv 5 \pmod{23}$

*Exercise 16.* Consider the modulus 23 and find all solutions  $x \in \mathbb{Z}$  to the following congruence  $69x \equiv 46 \pmod{23}$

*Exercise 17.* Let  $a, b, k$  be integers, such that  $a \equiv b \pmod{n}$  holds. Show  $a^k \equiv b^k \pmod{n}$ .

*Exercise 18.* Let  $a, n$  be integers, such that  $a$  and  $n$  are not coprime. For which  $b \in \mathbb{Z}$  does the congruence  $a \cdot x \equiv b \pmod{n}$  have a solution  $x$  and how does the solution set look in that case?

**The Chinese Remainder Theorem** We have seen how to solve congruencies in modular arithmetic. However, one question that remains is how to solve systems of congruencies with different moduli? The answer is given by the **Chinese reimainder theorem**, which states that

1217 for any  $k \in \mathbb{N}$  and coprime natural numbers  $n_1, \dots, n_k \in \mathbb{N}$  as well as integers  $a_1, \dots, a_k \in \mathbb{Z}$ , the  
 1218 so-called **simultaneous congruences**

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\dots \\ x &\equiv a_k \pmod{n_k} \end{aligned} \tag{3.15}$$

1219 has a solution, and all possible solutions of this congruence system are congruent modulo the  
 product  $N = n_1 \cdot \dots \cdot n_k$ .<sup>1</sup> In fact, the following algorithm computes the solution set:

check  
algorithm  
floating

---

**Algorithm 2** Chinese Remainder Theorem

---

**Require:**  $k \in \mathbb{Z}$ ,  $j \in \mathbb{N}_0$  and  $n_0, \dots, n_{k-1} \in \mathbb{N}$  coprime

**procedure** CONGRUENCE-SYSTEMS-SOLVER( $a_0, \dots, a_{k-1}$ )

$N \leftarrow n_0 \cdot \dots \cdot n_{k-1}$

**while**  $j < k$  **do**

$N_j \leftarrow N/n_j$

$(\_, s_j, t_j) \leftarrow \text{EXT-EUCLID}(N_j, n_j)$   $\triangleright 1 = s_j \cdot N_j + t_j \cdot n_j$

**end while**

$x' \leftarrow \sum_{j=0}^{k-1} a_j \cdot s_j \cdot N_j$

$x \leftarrow x' \bmod N$

**return**  $\{x + m \cdot N \mid m \in \mathbb{Z}\}$

**end procedure**

**Ensure:**  $\{x + m \cdot N \mid m \in \mathbb{Z}\}$  is the complete solution set to 3.15.

---

1220

*Example 8.* To illustrate how to solve simultaneous congruences using the Chinese remainder theorem, let's look at the following system of congruencies:

$$\begin{aligned} x &\equiv 4 \pmod{7} \\ x &\equiv 1 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 0 \pmod{11} \end{aligned}$$

Clearly all moduli are coprime and we have  $N = 7 \cdot 3 \cdot 5 \cdot 11 = 1155$ , as well as  $N_1 = 165$ ,  $N_2 = 385$ ,  $N_3 = 231$  and  $N_4 = 105$ . From this we calculate with the extended Euclidean algorithm

$$\begin{aligned} 1 &= 2 \cdot 165 + (-47) \cdot 7 \\ 1 &= 1 \cdot 385 + (-128) \cdot 3 \\ 1 &= 1 \cdot 231 + (-46) \cdot 5 \\ 1 &= 2 \cdot 105 + (-19) \cdot 11 \end{aligned}$$

1221 so we have  $x = 4 \cdot 2 \cdot 165 + 1 \cdot 1 \cdot 385 + 3 \cdot 1 \cdot 231 + 0 \cdot 2 \cdot 105 = 2398$  as one solution. Because  
 1222  $2398 \bmod 1155 = 88$  the set of all solutions is  $\{\dots, -2222, -1067, 88, 1243, 2398, \dots\}$ . We  
 1223 can invoke Sage's computation of the Chinese Remainder Theorem (CRT) to double check our  
 1224 findings:

1225 **sage:** CRT\_list([4, 1, 3, 0], [7, 3, 5, 11])

60

1226 **88**

61

---

<sup>1</sup>This is the classical Chinese remainder theorem as it was already known in ancient China. Under certain circumstances, the theorem can be extended to non-coprime moduli  $n_1, \dots, n_k$  but this is beyond the scope of this book. Interested readers should consult XXX [add references](#)

**Remainder Class Representation** As we have seen in various examples before, computing congruencies can be cumbersome and solution sets are large in general. It is therefore advantageous to find some kind of simplification for modular arithmetic.

Fortunately, this is possible and relatively straightforward once we identify each set of numbers with equal remainder with that remainder itself and call it the **remainder class** or **residue class** representation in modulo  $n$  arithmetic.

It then follows from the properties of Euclidean division that there are exactly  $n$  different remainder classes for every modulus  $n$  and that integer addition and multiplication can be projected to a new kind of addition and multiplication on those classes.

Roughly speaking, the new rules for addition and multiplication are then computed by taking any element of the first remainder class and some element of the second, then add or multiply them in the usual way and see which remainder class the result is contained in. The following example makes this abstract description more concrete:

*Example 9* (Arithmetic modulo 6). Choosing the modulus  $n = 6$ , we have six remainder classes of integers which are congruent modulo 6 (they have the same remainder when divided by 6) and when we identify each of those remainder classes with the remainder, we get the following identification:

$$\begin{aligned} 0 &:= \{\dots, -6, 0, 6, 12, \dots\} \\ 1 &:= \{\dots, -5, 1, 7, 13, \dots\} \\ 2 &:= \{\dots, -4, 2, 8, 14, \dots\} \\ 3 &:= \{\dots, -3, 3, 9, 15, \dots\} \\ 4 &:= \{\dots, -2, 4, 10, 16, \dots\} \\ 5 &:= \{\dots, -1, 5, 11, 17, \dots\} \end{aligned}$$

Now to compute the new addition law of those remainder class representatives, say  $2 + 5$ , one chooses arbitrary elements from both classes, say 14 and  $-1$ , adds those numbers in the usual way and then looks at the remainder class of the result.

So we get  $14 + (-1) = 13$ , and 13 is in the remainder class (of) 1. Hence we find that  $2 + 5 = 1$  in modular 6 arithmetic, which is a more readable way to write the congruence  $2 + 5 \equiv 1 \pmod{6}$ .

Applying the same reasoning to all remainder classes, addition and multiplication can be transferred to the representatives of the remainder classes. The results for modulus 6 arithmetic are summarized in the following addition and multiplication tables:

+	0	1	2	3	4	5	·	0	1	2	3	4	5
0	0	1	2	3	4	5	0	0	0	0	0	0	0
1	1	2	3	4	5	0	1	0	1	2	3	4	5
2	2	3	4	5	0	1	2	0	2	4	0	2	4
3	3	4	5	0	1	2	3	0	3	0	3	0	3
4	4	5	0	1	2	3	4	0	4	2	0	4	2
5	5	0	1	2	3	4	5	0	5	4	3	2	1

This way, we have defined a new arithmetic system that contains just 6 numbers and comes with its own definition of addition and multiplication. We call it **modular 6 arithmetic** and write the associated type as  $\mathbb{Z}_6$ .

To see why such an identification of a remainder class with its remainder is useful and actually simplifies congruence computations a lot, let's go back to the congruence from example 7 again:

$$7 \cdot (2x + 21) + 11 \equiv x - 102 \pmod{6} \quad (3.16)$$

1256 As shown in example 7, the arithmetic of congruencies can deviate from ordinary arithmetic:  
 1257 For example, division needs to check whether the modulus and the dividend are coprimes, and  
 1258 solutions are not unique in general.

We can rewrite this congruence as an **equation** over our new arithmetic type  $\mathbb{Z}_6$  by **projecting onto the remainder classes**. In particular, since  $7 \bmod 6 = 1$ ,  $21 \bmod 6 = 3$ ,  $11 \bmod 6 = 5$  and  $102 \bmod 6 = 0$  we have

$$7 \cdot (2x + 21) + 11 \equiv x - 102 \pmod{6} \text{ over } \mathbb{Z} \\ \Leftrightarrow 1 \cdot (2x + 3) + 5 = x \text{ over } \mathbb{Z}_6$$

1259 We can use the multiplication and addition table above to solves the equation on the right like  
 1260 we would solve normal integer equations:

$$\begin{array}{ll} 1 \cdot (2x + 3) + 5 = x & \\ 2x + 3 + 5 = x & \# \text{ addition-table: } 3 + 5 = 2 \\ 2x + 2 = x & \# \text{ add 4 and } -x \text{ on both sides} \\ 2x + 2 + 4 - x = x + 4 - x & \# \text{ addition-table: } 2 + 4 = 0 \\ x = 4 & \end{array}$$

1261 As we can see, despite the somewhat unfamiliar rules of addition and multiplication, solving  
 1262 congruencies this way is very similar to solving normal equations. And, indeed, the solution  
 1263 set is identical to the solution set of the original congruence, since 4 is identified with the set  
 1264  $\{4 + 6 \cdot k \mid k \in \mathbb{Z}\}$ .

1265 We can invoke Sage to do computations in our modular 6 arithmetic type. This is particularly  
 1266 useful to double-check our computations:

```
1267 sage: Z6 = Integers(6)                                     62
1268 sage: Z6(2) + Z6(5)                                       63
1269 1                                                         64
1270 sage: Z6(7) * (Z6(2) * Z6(4) + Z6(21)) + Z6(11) == Z6(4) - Z6(102) 65
1271 True                                                       66
```

1272 *Remark 2 (k-bit modulus).* In cryptographic papers, we sometimes read phrases like “[...] using  
 1273 a 4096-bit modulus”. This means that the underlying modulus  $n$  of the modular arithmetic used  
 1274 in the system has a binary representation with a length of 4096 bits. In contrast, the number 6  
 1275 has the binary representation 110 and hence our example 9 describes a 3-bit modulus arithmetic  
 1276 system.

1277 *Exercise 19.* Define  $\mathbb{Z}_{13}$  as the the arithmetic modulo 13 analog to example 9. Then consider  
 1278 the congruence from exercise 14 and rewrite it into an equation in  $\mathbb{Z}_{13}$

1279 **Modular Inverses** As we know, integers can be added, subtracted and multiplied so that the  
 1280 result is also an integer, but this is not true for the division of integers in general: for example,  
 1281  $3/2$  is not an integer anymore. To see why this is, from a more theoretical perspective, let us  
 1282 consider the definition of a multiplicative inverse first. When we have a set that has some kind  
 1283 of multiplication defined on it and we have a distinguished element of that set that behaves  
 1284 neutrally with respect to that multiplication (doesn’t change anything when multiplied with any  
 1285 other element), then we can define **multiplicative inverses** in the following way:

Let  $S$  be our set that has some notion  $a \cdot b$  of multiplication and a **neutral element**  $1 \in S$ , such that  $1 \cdot a = a$  for all elements  $a \in S$ . Then a **multiplicative inverse**  $a^{-1}$  of an element  $a \in S$  is defined as follows:

$$a \cdot a^{-1} = 1 \quad (3.17)$$

Informally speaking, the definition of a multiplicative inverse means that it “cancels” the original element to give 1 when they are multiplied.

Numbers that have multiplicative inverses are of particular interest, because they immediately lead to the definition of division by those numbers. In fact, if  $a$  is number such that the multiplicative inverse  $a^{-1}$  exists, then we define **division** by  $a$  simply as multiplication by the inverse:

$$\frac{b}{a} := b \cdot a^{-1} \quad (3.18)$$

*Example 10.* Consider the set of rational numbers, also known as fractions,  $\mathbb{Q}$ . For this set, the neutral element of multiplication is 1, since  $1 \cdot a = a$  for all rational numbers. For example,  $1 \cdot 4 = 4$ ,  $1 \cdot \frac{1}{4} = \frac{1}{4}$ , or  $1 \cdot 0 = 0$  and so on.

Every rational number  $a \neq 0$  has a multiplicative inverse, given by  $\frac{1}{a}$ . For example, the multiplicative inverse of 3 is  $\frac{1}{3}$ , since  $3 \cdot \frac{1}{3} = 1$ , the multiplicative inverse of  $\frac{5}{7}$  is  $\frac{7}{5}$ , since  $\frac{5}{7} \cdot \frac{7}{5} = 1$ , and so on.

*Example 11.* Looking at the set  $\mathbb{Z}$  of integers, we see that with respect to multiplication the neutral element is the number 1 and we notice that no integer other than 1 or  $-1$  has a multiplicative inverse, since the equation  $a \cdot x = 1$  has no integer solutions for  $a \neq 1$  or  $a \neq -1$ .

The definition of multiplicative inverse works verbatim for addition as well where it is called the additive inverse. In the case of integers, the neutral element with respect to addition is 0, since  $a + 0 = 0$  for all integers  $a \in \mathbb{Z}$ . The additive inverse always exist and is given by the negative number  $-a$ , since  $a + (-a) = 0$ .

*Example 12.* Looking at the set  $\mathbb{Z}_6$  of residual classes modulo 6 from example 9, we can use the multiplication table to find multiplicative inverses. To do so, we look at the row of the element and then find the entry equal to 1. If such an entry exists, the element of that column is the multiplicative inverse. If, on the other hand, the row has no entry equal to 1, we know that the element has no multiplicative inverse.

For example in  $\mathbb{Z}_6$  the multiplicative inverse of 5 is 5 itself, since  $5 \cdot 5 = 1$ . We can also see that 5 and 1 are the only elements that have multiplicative inverses in  $\mathbb{Z}_6$ .

Now, since 5 has a multiplicative inverse in modulo 6 arithmetic, we can divide by 5 in  $\mathbb{Z}_6$ , since we have a notation of multiplicative inverse and division is nothing but multiplication by the multiplicative inverse. For example

$$\frac{4}{5} = 4 \cdot 5^{-1} = 4 \cdot 5 = 2$$

From the last example, we can make the interesting observation that while 5 has no multiplicative inverse as an integer, it has a multiplicative inverse in modular 6 arithmetic.

This raises the question which numbers have multiplicative inverses in modular arithmetic. The answer is that, in modular  $n$  arithmetic, a number  $r$  has a multiplicative inverse, if and only if  $n$  and  $r$  are coprime. Since  $\gcd(n, r) = 1$  in that case, we know from the extended Euclidean algorithm that there are numbers  $s$  and  $t$ , such that

$$1 = s \cdot n + t \cdot r \quad (3.19)$$

If we take the modulus  $n$  on both sides, the term  $s \cdot n$  vanishes, which tells us that  $t \bmod n$  is the multiplicative inverse of  $r$  in modular  $n$  arithmetic.

*Example 13* (Multiplicative inverses in  $\mathbb{Z}_6$ ). In the previous example, we looked up multiplicative inverses in  $\mathbb{Z}_6$  from the lookup-table in Example 9. In real world examples, it is usually impossible to write down those lookup tables, as the modulus is way too large, and the sets occasionally contain more elements than there are atoms in the observable universe.

Now, trying to determine that  $2 \in \mathbb{Z}_6$  has no multiplicative inverse in  $\mathbb{Z}_6$  without using the lookup table, we immediately observe that 2 and 6 are not coprime, since their greatest common divisor is 2. It follows that equation 3.19 has no solutions  $s$  and  $t$ , which means that 2 has no multiplicative inverse in  $\mathbb{Z}_6$ .

The same reasoning works for 3 and 4, as neither of these are coprime with 6. The case of 5 is different, since  $\gcd(6, 5) = 1$ . To compute the multiplicative inverse of 5, we use the extended Euclidean algorithm and compute the following:

k	$r_k$	$s_k$	$t_k = (r_k - s_k \cdot a) \div b$
0	6	1	0
1	5	0	1
2	1	1	-1
3	0	.	.

We get  $s = 1$  as well as  $t = -1$  and have  $1 = 1 \cdot 6 - 1 \cdot 5$ . From this, it follows that  $-1 \bmod 6 = 5$  is the multiplicative inverse of 5 in modular 6 arithmetic. We can double check using Sage:

```
sage: ZZ(6).xgcd(ZZ(5))
(1, 1, -1)
```

67

68

At this point, the attentive reader might notice that the situation where the modulus is a prime number is of particular interest, because we know from exercise 8 that in these cases all remainder classes must have modular inverses, since  $\gcd(r, n) = 1$  for prime  $n$  and any  $r < n$ . In fact, Fermat's little theorem provides a way to compute multiplicative inverses in this situation, since in case of a prime modulus  $p$  and  $r < p$ , we get the following:

$$\begin{aligned} r^p &\equiv r \pmod{p} \Leftrightarrow \\ r^{p-1} &\equiv 1 \pmod{p} \Leftrightarrow \\ r \cdot r^{p-2} &\equiv 1 \pmod{p} \end{aligned}$$

This tells us that the multiplicative inverse of a residue class  $r$  in modular  $p$  arithmetic is precisely  $r^{p-2}$ .

*Example 14* (Modular 5 arithmetic). To see the unique properties of modular arithmetic when the modulus is a prime number, we will replicate our findings from example 9, but this time for the prime modulus 5. For  $n = 5$  we have five equivalence classes of integers which are congruent modulo 5. We write this as follows:

$$\begin{aligned} 0 &:= \{\dots, -5, 0, 5, 10, \dots\} \\ 1 &:= \{\dots, -4, 1, 6, 11, \dots\} \\ 2 &:= \{\dots, -3, 2, 7, 12, \dots\} \\ 3 &:= \{\dots, -2, 3, 8, 13, \dots\} \\ 4 &:= \{\dots, -1, 4, 9, 14, \dots\} \end{aligned}$$

Addition and multiplication can be transferred to the equivalence classes, in a way exactly parallel to Example 9. This results in the following addition and multiplication tables:



1343

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

1344 Calling the set of remainder classes in modular 5 arithmetic with this addition and multiplication  
 1345  $\mathbb{Z}_5$ , we see some subtle but important differences to the situation in  $\mathbb{Z}_6$ . In particular, we see  
 1346 that in the multiplication table, every remainder  $r \neq 0$  has the entry 1 in its row and therefore  
 1347 has a multiplicative inverse. In addition, there are no non-zero elements such that their product  
 1348 is zero.

1349 To use Fermat's little theorem in  $\mathbb{Z}_5$  for computing multiplicative inverses (instead of using  
 1350 the multiplication table), let's consider  $3 \in \mathbb{Z}_5$ . We know that the multiplicative inverse is given  
 1351 by the remainder class that contains  $3^{5-2} = 3^3 = 3 \cdot 3 \cdot 3 = 4 \cdot 3 = 2$ . And indeed  $3^{-1} = 2$ , since  
 1352  $3 \cdot 2 = 1$  in  $\mathbb{Z}_5$ .

1353 We can invoke Sage to do computations in our modular 5 arithmetic type to double-check  
 1354 our computations:

```

1355 sage: Z5 = Integers(5)                                69
1356 sage: Z5(3) ** (5-2)                                    70
1357 2                                                         71
1358 sage: Z5(3) ** (-1)                                     72
1359 2                                                         73
1360 sage: Z5(3) ** (5-2) == Z5(3) ** (-1)                  74
1361 True                                                    75

```

*Example 15.* To understand one of the principal differences between prime number modular arithmetic and non-prime number modular arithmetic, consider the linear equation  $a \cdot x + b = 0$  defined over both types  $\mathbb{Z}_5$  and  $\mathbb{Z}_6$ . Since in  $\mathbb{Z}_5$  every non-zero element has a multiplicative inverse, we can always solve these equations in  $\mathbb{Z}_5$ , which is not true in  $\mathbb{Z}_6$ . To see that, consider the equation  $3x + 3 = 0$ . In  $\mathbb{Z}_5$  we have the following:

$$\begin{array}{ll}
 3x + 3 = 0 & \# \text{ add 2 and on both sides} \\
 3x + 3 + 2 = 2 & \# \text{ addition-table: } 2 + 3 = 0 \\
 3x = 2 & \# \text{ divide by 3 (which equals multiplication by 2)} \\
 2 \cdot (3x) = 2 \cdot 2 & \# \text{ multiplication-table: } 2 \cdot 2 = 4 \\
 x = 4 &
 \end{array}$$

So in the case of our prime number modular arithmetic, we get the unique solution  $x = 4$ . Now consider  $\mathbb{Z}_6$ :

$$\begin{array}{ll}
 3x + 3 = 0 & \# \text{ add 3 and on both sides} \\
 3x + 3 + 3 = 3 & \# \text{ addition-table: } 3 + 3 = 0 \\
 3x = 3 & \# \text{ division not possible (no multiplicative inverse of 3 exists)}
 \end{array}$$

1362 So, in this case, we cannot solve the equation for  $x$  by dividing by 3. And, indeed, when we look  
 1363 at the multiplication table of  $\mathbb{Z}_6$  (Example 9), we find that there are three solutions  $x \in \{1, 3, 5\}$ ,  
 1364 such that  $3x + 3 = 0$  holds true for all of them.

1365 *Exercise 20.* Consider the modulus  $n = 24$ . Which of the integers 7, 1, 0, 805,  $-4255$  have  
 1366 multiplicative inverses in modular 24 arithmetic? Compute the inverses, in case they exist.

1367 *Exercise 21.* Find the set of all solutions to the congruence  $17(2x + 5) - 4 \equiv 2x + 4 \pmod{5}$ .  
 1368 Then project the congruence into  $\mathbb{Z}_5$  and solve the resulting equation in  $\mathbb{Z}_5$ . Compare the results.

1369 *Exercise 22.* Find the set of all solutions to the congruence  $17(2x + 5) - 4 \equiv 2x + 4 \pmod{6}$ .  
 1370 Then project the congruence into  $\mathbb{Z}_6$  and try to solve the resulting equation in  $\mathbb{Z}_6$ .

### 1371 3.4 Polynomial arithmetic

1372 A polynomial is an expression consisting of variables (also called indeterminates) and coeffi-  
 1373 cients that involves only the operations of addition, subtraction and multiplication. All coeffi-  
 1374 cients of a polynomial must have the same type, e.g. being integers or rational numbers etc. To  
 1375 be more precise an *univariate polynomial* is an expression

$$P(x) := \sum_{j=0}^m a_j x^j = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0, \quad (3.20)$$

1376 where  $x$  is called the **indeterminate**, each  $a_j$  is called a **coefficient**. If  $R$  is the type of the  
 1377 coefficients, then the set of all **univariate<sup>2</sup> polynomials with coefficients in  $R$**  is written as  
 1378  $R[x]$ . We often simply use **polynomial** instead of univariate polynomial, write  $P(x) \in R[x]$  for a  
 1379 polynomial and denote the constant term  $a_0$  as  $P(0)$ .

1380 A polynomial is called the **zero polynomial** if all coefficients are zero and a polynomial is  
 1381 called the **one polynomial** if the constant term is 1 and all other coefficients are zero.

1382 Given an univariate polynomial  $P(x) = \sum_{j=0}^m a_j x^j$  that is not the zero polynomial, we call the  
 1383 non-negative integer  $\deg(P) := m$  the *degree* of  $P$  and define the degree of the zero polynomial  
 1384 to be  $-\infty$ , where  $-\infty$  (negative infinity) is a symbol with the properties that  $-\infty + m = -\infty$  and  
 1385  $-\infty < m$  for all non-negative integers  $m \in \mathbb{N}_0$ . In addition, we write

$$Lc(P) := a_m \quad (3.21)$$

1386 and call it the **leading coefficient** of the polynomial  $P$ . We can restrict the set  $R[x]$  of **all**  
 1387 polynomials with coefficients in  $R$ , to the set of all such polynomials that have a degree that  
 1388 does not exceed a certain value. If  $m$  is the maximum degree allowed, we write  $R_{\leq m}[x]$  for the  
 1389 set of all polynomials with a degree less than or equal to  $m$ .

*Example 16* (Integer Polynomials). The coefficients of a polynomial must all have the same type. The set of polynomials with integer coefficients is written as  $\mathbb{Z}[x]$ . Examples of such polynomials are:

$P_1(x) = 2x^2 - 4x + 17$	# with $\deg(P_1) = 2$ and $Lc(P_1) = 2$
$P_2(x) = x^{23}$	# with $\deg(P_2) = 23$ and $Lc(P_2) = 1$
$P_3(x) = x$	# with $\deg(P_3) = 1$ and $Lc(P_3) = 1$
$P_4(x) = 174$	# with $\deg(P_4) = 0$ and $Lc(P_4) = 174$
$P_5(x) = 1$	# with $\deg(P_5) = 0$ and $Lc(P_5) = 1$
$P_6(x) = 0$	# with $\deg(P_6) = -\infty$ and $Lc(P_6) = 0$
$P_7(x) = (x - 2)(x + 3)(x - 5)$	

---

<sup>2</sup>in our context the term univariate means that the polynomial contains a single variable only

In particular, every integer can be seen as an integer polynomial of degree zero.  $P_7$  is a polynomial, because we can expand its definition into  $P_7(x) = x^3 - 4x^2 - 11x + 30$ , which is a polynomial of degree 3 and leading coefficient 1. The following expressions are not integer polynomials:

$$Q_1(x) = 2x^2 + 4 + 3x^{-2}$$

$$Q_2(x) = 0.5x^4 - 2x$$

$$Q_3(x) = 2^x$$

1390 In particular  $Q_1$  is not an integer polynomial, because the expression  $x^{-2}$  has a negative expo-  
 1391 nent,  $Q_2$  is not an integer polynomial because the coefficient 0.5 is not an integer and  $Q_3$  is not  
 1392 an integer polynomial because the indeterminant appears in the exponent of of a coefficient.

1393 We can invoke Sage to do computations with polynomials. To do so, we have to specify the  
 1394 symbol for the indeterminate and the type for the coefficients (For the definition of rings see  
 1395 4.2). Note, however that Sage defines the degree of the zero polynomial to be  $-1$ .

```

1396 sage: Zx = ZZ['x'] # integer polynomials with indeterminate x 76
1397 sage: Zt.<t> = ZZ[] # integer polynomials with indeterminate t 77
1398 sage: Zx 78
1399 Univariate Polynomial Ring in x over Integer Ring 79
1400 sage: Zt 80
1401 Univariate Polynomial Ring in t over Integer Ring 81
1402 sage: p1 = Zx([17,-4,2]) 82
1403 sage: p1 83
1404 2*x^2 - 4*x + 17 84
1405 sage: p1.degree() 85
1406 2 86
1407 sage: p1.leading_coefficient() 87
1408 2 88
1409 sage: p2 = Zt(t^23) 89
1410 sage: p2 90
1411 t^23 91
1412 sage: p6 = Zx([0]) 92
1413 sage: p6.degree() 93
1414 -1 94

```

*Example 17* (Polynomials over  $\mathbb{Z}_6$ ). Recall the definition of modular 6 arithmetics  $\mathbb{Z}_6$  as defined in example 9. The set of all polynomials with indeterminate  $x$  and coefficients in  $\mathbb{Z}_6$  is symbolized as  $\mathbb{Z}_6[x]$ . Example of polynomials from  $\mathbb{Z}_6[x]$  are:

$P_1(x) = 2x^2 - 4x + 5$	# with $\deg(P_1) = 2$ and $Lc(P_1) = 2$
$P_2(x) = x^{23}$	# with $\deg(P_2) = 23$ and $Lc(P_2) = 1$
$P_3(x) = x$	# with $\deg(P_3) = 1$ and $Lc(P_3) = 1$
$P_4(x) = 3$	# with $\deg(P_4) = 0$ and $Lc(P_4) = 3$
$P_5(x) = 1$	# with $\deg(P_5) = 0$ and $Lc(P_5) = 1$
$P_6(x) = 0$	# with $\deg(P_5) = -\infty$ and $Lc(P_6) = 0$
$P_7(x) = (x-2)(x+3)(x-5)$	

Just like in the previous example,  $P_7$  is a polynomial. However, since we are working with coefficients from  $\mathbb{Z}_6$  now the expansion of  $P_7$  is computed differently, as we have to invoke addition and multiplication in  $\mathbb{Z}_6$  as defined in XXX. We get the following:

$$\begin{aligned}
 (x-2)(x+3)(x-5) &= (x+4)(x+3)(x+1) && \# \text{ additive inverses in } \mathbb{Z}_6 \\
 &= (x^2 + 4x + 3x + 3 \cdot 4)(x+1) && \# \text{ bracket expansion} \\
 &= (x^2 + 1x + 0)(x+1) && \# \text{ computation in } \mathbb{Z}_6 \\
 &= x^3 + x^2 + x^2 + x && \# \text{ bracket expansion} \\
 &= x^3 + 2x^2 + x
 \end{aligned}$$

1415 Again, we can use Sage to do computations with polynomials that have their coefficients in  $\mathbb{Z}_6$   
 1416 (For the definition of rings see 4.2). To do so, we have to specify the symbol for the indertemi-  
 1417 nate and the type for the coefficients:

```

1418 sage: Z6 = Integers(6)                                     95
1419 sage: Z6x = Z6['x']                                         96
1420 sage: Z6x                                                    97
1421 Univariate Polynomial Ring in x over Ring of integers modulo 6 98
1422 sage: p1 = Z6x([5,-4,2])                                     99
1423 sage: p1                                                    100
1424 2*x^2 + 2*x + 5                                             101
1425 sage: p1 = Z6x([17,-4,2])                                    102
1426 sage: p1                                                    103
1427 2*x^2 + 2*x + 5                                             104
1428 sage: Z6x(x-2)*Z6x(x+3)*Z6x(x-5) == Z6x(x^3 + 2*x^2 + x) 105
1429 True                                                         106

```

1430 Given some element from the same type as the coefficients of a polynomial, the polyno-  
 1431 mial can be evaluated at that element, which means that we insert the given element for every  
 1432 occurrence of the indeterminate  $x$  in the polynomial expression.

1433 To be more precise, let  $P \in R[x]$ , with  $P(x) = \sum_{j=0}^m a_j x^j$  be a polynomial with a coefficient  
 1434 of type  $R$  and let  $b \in R$  be an element of that type. Then the **evaluation** of  $P$  at  $b$  is given as  
 1435 follows:

$$P(b) = \sum_{j=0}^m a_j b^j \quad (3.22)$$

*Example 18.* Consider the integer polynomials from example 16 again. To evaluate them at given points, we have to insert the point for all occurrences of  $x$  in the polynomial expression. Inserting arbitrary values from  $\mathbb{Z}$ , we get:

$$\begin{aligned}
 P_1(2) &= 2 \cdot 2^2 - 4 \cdot 2 + 17 = 17 \\
 P_2(3) &= 3^{23} = 94143178827 \\
 P_3(-4) &= -4 = -4 \\
 P_4(15) &= 174 \\
 P_5(0) &= 1 \\
 P_6(1274) &= 0 \\
 P_7(-6) &= (-6-2)(-6+3)(-6-5) = -264
 \end{aligned}$$

1436 Note, however, that it is not possible to evaluate any of those polynomial on values of different  
 1437 type. For example, it is not strictly correct to write  $P_1(0.5)$ , since 0.5 is not an integer. We can  
 1438 verify our computations using Sage:

```

1439 sage: Zx = ZZ['x']                                     107
1440 sage: p1 = Zx([17, -4, 2])                             108
1441 sage: p7 = Zx(x-2)*Zx(x+3)*Zx(x-5)                   109
1442 sage: p1(ZZ(2))                                       110
1443 17                                                    111
1444 sage: p7(ZZ(-6)) == ZZ(-264)                         112
1445 True                                                  113

```

*Example 19.* Consider the polynomials with coefficients in  $\mathbb{Z}_6$  from example again. To evaluate them at given values from  $\mathbb{Z}_6$ , we have to insert the point for all occurrences of  $x$  in the polynomial expression. We get the following:

$$\begin{aligned}
 P_1(2) &= 2 \cdot 2^2 - 4 \cdot 2 + 5 = 2 - 2 + 5 = 5 \\
 P_2(3) &= 3^{23} = 3 \\
 P_3(-4) &= P_3(2) = 2 \\
 P_5(0) &= 1 \\
 P_6(4) &= 0
 \end{aligned}$$

```

1446
1447 sage: Z6 = Integers(6)                                 114
1448 sage: Z6x = Z6['x']                                    115
1449 sage: p1 = Z6x([5, -4, 2])                             116
1450 sage: p1(Z6(2)) == Z6(5)                               117
1451 True                                                  118

```

1452 *Exercise 23.* Compare both expansions of  $P_7$  from  $\mathbb{Z}[x]$  and from  $\mathbb{Z}_6[x]$  in example 16 and  
 1453 example 19, and consider the definition of  $\mathbb{Z}_6$  as given in example 9. Can you see how the  
 1454 definition of  $P_7$  over  $\mathbb{Z}$  projects to the definition over  $\mathbb{Z}_6$  if you consider the residue classes of  
 1455  $\mathbb{Z}_6$ ?

1456 **Polynomial arithmetic** Polynomials behave like integers in many ways. In particular, they  
 1457 can be added, subtracted and multiplied. In addition, they have their own notion of Euclidean  
 1458 division. Informally speaking, we can add two polynomials by simply adding the coefficients  
 1459 of the same index, and we can multiply them by applying the distributive property, that is, by  
 1460 multiplying every term of the left factor with every term of the right factor and adding the results  
 1461 together.

1462 To be more precise let  $\sum_{n=0}^{m_1} a_n x^n$  and  $\sum_{n=0}^{m_2} b_n x^n$  be two polynomials from  $R[x]$ . Then the  
 1463 **sum** and the **product** of these polynomials is defined as follows:

$$\sum_{n=0}^{m_1} a_n x^n + \sum_{n=0}^{m_2} b_n x^n = \sum_{n=0}^{\max\{m_1, m_2\}} (a_n + b_n) x^n \quad (3.23)$$

$$\left( \sum_{n=0}^{m_1} a_n x^n \right) \cdot \left( \sum_{n=0}^{m_2} b_n x^n \right) = \sum_{n=0}^{m_1+m_2} \sum_{i=0}^n a_i b_{n-i} x^n \quad (3.24)$$

A rule for polynomial subtraction can be deduced from these two rules by first multiplying the **subtrahend** with (the polynomial)  $-1$  and then add the result to the **minuend**.

subtrahend

Regarding the definition of the degree of a polynomial, we see that the degree of the sum is always the maximum of the degrees of both summands, and the degree of the product is always the degree of the sum of the factors, since we defined  $-\infty + m = -\infty$  for every integer  $m \in \mathbb{Z}$ .

minuend

*Example 20.* To give an example of how polynomial arithmetic works, consider the following two integer polynomials  $P, Q \in \mathbb{Z}[x]$  with  $P(x) = 5x^2 - 4x + 2$  and  $Q(x) = x^3 - 2x^2 + 5$ . The sum of these two polynomials is computed by adding the coefficients of each term with equal exponent in  $x$ . This gives the following:

$$\begin{aligned}(P + Q)(x) &= (0 + 1)x^3 + (5 - 2)x^2 + (-4 + 0)x + (2 + 5) \\ &= x^3 + 3x^2 - 4x + 7\end{aligned}$$

The product of these two polynomials is computed by multiplication of each term in the first factor with each term in the second factor. We get the following:

$$\begin{aligned}(P \cdot Q)(x) &= (5x^2 - 4x + 2) \cdot (x^3 - 2x^2 + 5) \\ &= (5x^5 - 10x^4 + 25x^2) + (-4x^4 + 8x^3 - 20x) + (2x^3 - 4x^2 + 10) \\ &= 5x^5 - 14x^4 + 10x^3 + 21x^2 - 20x + 10\end{aligned}$$

```

1471 sage: Zx = ZZ['x']
1472 sage: P = Zx([2, -4, 5])
1473 sage: Q = Zx([5, 0, -2, 1])
1474 sage: P+Q == Zx(x^3 + 3*x^2 - 4*x + 7)
1475 True
1476 sage: P*Q == Zx(5*x^5 - 14*x^4 + 10*x^3 + 21*x^2 - 20*x + 10)
1477 True

```

*Example 21.* Let us consider the polynomials of the previous example but interpreted in modular 6 arithmetic. So we consider  $P, Q \in \mathbb{Z}_6[x]$  again with  $P(x) = 5x^2 - 4x + 2$  and  $Q(x) = x^3 - 2x^2 + 5$ . This time we get the following:

$$\begin{aligned}(P + Q)(x) &= (0 + 1)x^3 + (5 - 2)x^2 + (-4 + 0)x + (2 + 5) \\ &= (0 + 1)x^3 + (5 + 4)x^2 + (2 + 0)x + (2 + 5) \\ &= x^3 + 3x^2 + 2x + 1\end{aligned}$$

$$\begin{aligned}(P \cdot Q)(x) &= (5x^2 - 4x + 2) \cdot (x^3 - 2x^2 + 5) \\ &= (5x^2 + 2x + 2) \cdot (x^3 + 4x^2 + 5) \\ &= (5x^5 + 2x^4 + 1x^2) + (2x^4 + 2x^3 + 4x) + (2x^3 + 2x^2 + 4) \\ &= 5x^5 + 4x^4 + 4x^3 + 3x^2 + 4x + 4\end{aligned}$$

```

1478
1479 sage: Z6x = Integers(6)['x']
1480 sage: P = Z6x([2, -4, 5])

```

```

1481 sage: Q = Z6x([5, 0, -2, 1]) 128
1482 sage: P+Q == Z6x(x^3 +3*x^2 +2*x +1) 129
1483 True 130
1484 sage: P*Q == Z6x(5*x^5 +4*x^4 +4*x^3+3*x^2+4*x +4) 131
1485 True 132

```

1486 *Exercise 24.* Compare the sum  $P + Q$  and the product  $P \cdot Q$  from the previous two examples  
 1487 20 and 21 and consider the definition of  $\mathbb{Z}_6$  as given in example 9. How can we derive the  
 1488 computations in  $\mathbb{Z}_6[x]$  from the computations in  $\mathbb{Z}[x]$ ?

1489 **Euklidean Division** The arithmetic of polynomials share a lot of properties with the arith-  
 1490 metic of integers and as a consequence the concept of Euclidean division and the algorithm of  
 1491 long division is also defined for polynomials. Recalling the Euclidean division of integers 3.2,  
 1492 we know that, given two integers  $a$  and  $b \neq 0$ , there is always another integer  $m$  and a natural  
 1493 number  $r$  with  $r < |b|$  such that  $a = m \cdot b + r$  holds.

1494 We can generalize this to polynomials whenever the leading coefficient of the dividend  
 1495 polynomial has a notion of multiplicative inverse. In fact, given two polynomials  $A$  and  $B \neq 0$   
 1496 from  $R[x]$  such that  $Lc(B)^{-1}$  exists in  $R$ , there exist two polynomials  $Q$  (the quotient) and  $P$  (the  
 1497 remainder), such that the following equation holds:

$$A = Q \cdot B + P \quad (3.25)$$

1498 and  $\deg(P) < \deg(B)$ . Similarly to integer Euclidean division, both  $Q$  and  $P$  are uniquely  
 1499 defined by these relations.

1500 *Notation and Symbols 2.* Suppose that the polynomials  $A, B, Q$  and  $P$  satisfy equation 3.25. We  
 1501 often use the following notation to describe the quotient and the remainder polynomials of the  
 1502 Euclidean division:

$$A \operatorname{div} B := Q, \quad A \operatorname{mod} B := P \quad (3.26)$$

1503 We also say that a polynomial  $A$  is divisible by another polynomial  $B$  if  $A \operatorname{mod} B = 0$  holds. In  
 1504 this case, we also write  $B|A$  and call  $B$  a *factor* of  $A$ .

1505 Analogously to integers, methods to compute Euclidean division for polynomials are called  
 1506 **polynomial division algorithms**. Probably the best known algorithm is the so called **polyno-**  
 1507 **mial long division**.

1508 This algorithm works only when there is a notion of division by the leading coefficient of  $B$ .  
 1509 It can be generalized, but we will only need this somewhat simpler method in what follows.

1510 *Example 22* (Polynomial Long Division). To give an example of how the previous algorithm  
 1511 works, let us divide the integer polynomial  $A(x) = x^5 + 2x^3 - 9 \in \mathbb{Z}[x]$  by the integer polynomial  
 1512  $B(x) = x^2 + 4x - 1 \in \mathbb{Z}[x]$ . Since  $B$  is not the zero polynomial and the leading coefficient of  $B$   
 1513 is 1, which is invertible as an integer, we can apply algorithm 1. Our goal is to find solutions  
 1514 to equation XXX, that is, we need to find the quotient polynomial  $Q \in \mathbb{Z}[x]$  and the remainder  
 1515 polynomial  $P \in \mathbb{Z}[x]$  such that  $x^5 + 2x^3 - 9 = Q(x) \cdot (x^2 + 4x - 1) + P(x)$ . Using a notation that

algorithm-  
floating

---

**Algorithm 3** Polynomial Euclidean Algorithm

**Require:**  $A, B \in R[x]$  with  $B \neq 0$ , such that  $Lc(B)^{-1}$  exists in  $R$

**procedure** POLY-LONG-DIVISION( $A, B$ )

$$Q \leftarrow 0$$
$$P \leftarrow A$$
$$d \leftarrow \deg(B)$$
$$c \leftarrow Lc(B)$$
**while**  $\deg(P) \geq d$  **do**
$$S := Lc(P) \cdot c^{-1} \cdot x^{\deg(P)-d}$$
$$Q \leftarrow Q + S$$
$$P \leftarrow P - S \cdot B$$
**end while****return**  $(Q, P)$ 

**end procedure**

**Ensure:**  $A = Q \cdot B + P$

1516 is mostly used in anglophone countries, we compute as follows:

$$\begin{array}{r}
 \phantom{X^2+4X-1)} \phantom{X^5} X^3 - 4X^2 + 19X - 80 \\
 \phantom{X^2+4X-1)} \phantom{X^5} \phantom{X^4} + 2X^3 \phantom{+ 19X - 80} - 9 \\
 \phantom{X^2+4X-1)} \phantom{X^5} - X^5 - 4X^4 + X^3 \\
 \hline
 \phantom{X^2+4X-1)} \phantom{X^5} - 4X^4 + 3X^3 \\
 \phantom{X^2+4X-1)} \phantom{X^5} 4X^4 + 16X^3 - 4X^2 \\
 \hline
 \phantom{X^2+4X-1)} \phantom{X^5} \phantom{X^4} 19X^3 - 4X^2 \\
 \phantom{X^2+4X-1)} \phantom{X^5} - 19X^3 - 76X^2 + 19X \\
 \hline
 \phantom{X^2+4X-1)} \phantom{X^5} \phantom{X^4} \phantom{X^3} - 80X^2 + 19X - 9 \\
 \phantom{X^2+4X-1)} \phantom{X^5} \phantom{X^4} \phantom{X^3} 80X^2 + 320X - 80 \\
 \hline
 \phantom{X^2+4X-1)} \phantom{X^5} \phantom{X^4} \phantom{X^3} \phantom{X^2} 339X - 89
 \end{array}
 \tag{3.27}$$

We therefore get  $Q(x) = x^3 - 4x^2 + 19x - 80$  as well as  $P(x) = 339x - 89$  and indeed we have  $x^5 + 2x^3 - 9 = (x^3 - 4x^2 + 19x - 80) \cdot (x^2 + 4x - 1) + (339x - 89)$ , which we can double check invoking Sage:

```

1520 sage: Zx = ZZ['x'] 133
1521 sage: A = Zx([-9, 0, 0, 2, 0, 1]) 134
1522 sage: B = Zx([-1, 4, 1]) 135
1523 sage: Q = Zx([-80, 19, -4, 1]) 136
1524 sage: P = Zx([-89, 339]) 137
1525 sage: A == Q*B + P 138
1526 True 139

```

Example 23. In the previous example, polynomial division gave a non-trivial (non-vanishing, i.e non-zero) remainder. Of special interest are divisions that don't give a remainder. Such divisors are called factors of the dividend.

For example, consider the integer polynomial  $P_7$  from example 16 again. As we have shown, it can be written both as  $x^3 - 4x^2 - 11x + 30$  and as  $(x - 2)(x + 3)(x - 5)$ . From this, we can see that the polynomials  $F_1(x) = (x - 2)$ ,  $F_2(x) = (x + 3)$  and  $F_3(x) = (x - 5)$  are all factors of  $x^3 - 4x^2 - 11x + 30$ , since division of  $P_7$  by any of these factors will result in a zero remainder.



1534 *Exercise 25.* Consider the polynomial expressions  $A(x) := -3x^4 + 4x^3 + 2x^2 + 4$  and  $B(x) =$   
 1535  $x^2 - 4x + 2$ . Compute the Euclidean division of  $A$  by  $B$  in the following types:

1536 1.  $A, B \in \mathbb{Z}[x]$

1537 2.  $A, B \in \mathbb{Z}_6[x]$

1538 3.  $A, B \in \mathbb{Z}_5[x]$

1539 Now consider the result in  $\mathbb{Z}[x]$  and in  $\mathbb{Z}_6[x]$ . How can we compute the result in  $\mathbb{Z}_6[x]$  from the  
 1540 result in  $\mathbb{Z}[x]$ ?

1541 *Exercise 26.* Show that the polynomial  $B(x) = 2x^4 - 3x + 4 \in \mathbb{Z}_5[x]$  is a factor of the polynomial  
 1542  $A(x) = x^7 + 4x^6 + 4x^5 + x^3 + 2x^2 + 2x + 3 \in \mathbb{Z}_5[x]$  that is show  $B|A$ . What is  $B \operatorname{div} A$ ?

1543 **Prime Factors** Recall that the fundamental theorem of arithmetic 3.6 tells us that every natu-  
 1544 ral number is the product of prime numbers. In this chapter we will see that something similar  
 1545 holds for univariate polynomials  $R[x]$ , too<sup>3</sup>.

1546 The polynomial analog to a prime number is a so called an **irreducible polynomial**, which  
 1547 is defined as a polynomial that cannot be factored into the product of two non-constant poly-  
 1548 nomials using Euclidean division. Irreducible polynomials are for polynomials what prime  
 1549 numbers are for integer: They are the basic building blocks from which all other polynomials  
 1550 can be constructed. To be more precise, let  $P \in R[x]$  be any polynomial. Then there are always  
 1551 irreducible polynomials  $F_1, F_2, \dots, F_k \in R[x]$ , such that the following holds:

$$P = F_1 \cdot F_2 \cdot \dots \cdot F_k. \quad (3.28)$$

1552 This representation is unique, except for permutations in the factors and is called the **prime**  
 1553 **factorization** of  $P$ . Moreover each factor  $F_i$  is called a **prime factor** of  $P$ .

1554 *Example 24.* Consider the polynomial expression  $P = x^2 - 3$ . When we interpret  $P$  as an integer  
 1555 polynomial  $P \in \mathbb{Z}[x]$ , we find that this polynomial is irreducible, since any factorization other  
 1556 then  $1 \cdot (x^2 - 3)$ , must look like  $(x - a)(x + a)$  for some integer  $a$ , but there is no integers  $a$  with  
 1557  $a^2 = 3$ .

1558	<b>sage:</b> <code>Zx = ZZ['x']</code>	140
1559	<b>sage:</b> <code>p = Zx(x^2-3)</code>	141
1560	<b>sage:</b> <code>p.factor()</code>	142
1561	<code>x^2 - 3</code>	143

1562 On the other hand interpreting  $P$  as a polynomial  $P \in \mathbb{Z}_6[x]$  in modulo 6 arithmetic, we see that  $P$   
 1563 has two factors  $F_1 = (x - 3)$  and  $F_2 = (x + 3)$ , since  $(x - 3)(x + 3) = x^2 - 3x + 3x - 3 \cdot 3 = x^2 - 3$ .

1564 Points where a polynomial evaluates to zero are called **roots** of the polynomial. To be more  
 1565 precise, let  $P \in R[x]$  be a polynomial. Then a root is a point  $x_0 \in R$  with  $P(x_0) = 0$  and the set  
 1566 of all roots of  $P$  is defined as follows:

$$R_0(P) := \{x_0 \in R \mid P(x_0) = 0\} \quad (3.29)$$

1567 The roots of a polynomial are of special interest with respect to it's prime factorization, since it  
 1568 can be shown that for any given root  $x_0$  of  $P$  the polynomial  $F(x) = (x - x_0)$  is a prime factor of  
 1569  $P$ .

---

<sup>3</sup>Strictly speaking this is not true for polynomials over arbitrary types  $R$ . However in this book we assume  $R$  to be a so called unique factorization domain for which the content of this section holds.

Finding the roots of a polynomial is sometimes called **solving the polynomial**. It is a hard problem and has been the subject of much research throughout history.

It can be shown that if  $m$  is the degree of a polynomial  $P$ , then  $P$  can not have more than  $m$  roots. However, in general, polynomials can have less than  $m$  roots.

*Example 25.* Consider the integer polynomial  $P_7(x) = x^3 - 4x^2 - 11x + 30$  from example 16 again. We know that its set of roots is given by  $R_0(P_7) = \{-3, 2, 5\}$ .

On the other hand, we know from example 24 that the integer polynomial  $x^2 - 3$  is irreducible. It follows that it has no roots, since every root defines a prime factor.

*Example 26.* To give another example, consider the integer polynomial  $P = x^7 + 3x^6 + 3x^5 + x^4 - x^3 - 3x^2 - 3x - 1$ . We can invoke Sage to compute the roots and prime factors of  $P$ :

```
sage: Zx = ZZ['x']
sage: p = Zx(x^7 + 3*x^6 + 3*x^5 + x^4 - x^3 - 3*x^2 - 3*x - 1)
sage: p.roots()
[(1, 1), (-1, 4)]
sage: p.factor()
(x - 1) * (x + 1)^4 * (x^2 + 1)
```

We see that  $P$  has the root 1 and that the associated prime factor  $(x - 1)$  occurs once in  $P$  and that it has the root  $-1$ , where the associated prime factor  $(x + 1)$  occurs 4 times in  $P$ . This gives the following prime factorization:

$$P = (x - 1)(x + 1)^4(x^2 + 1)$$

*Exercise 27.* Show that if a polynomial  $P \in R[x]$  of degree  $\deg(P) = m$  has less than  $m$  roots, it must have a prime factor  $F$  of degree  $\deg(F) > 1$ .

*Exercise 28.* Consider the polynomial  $P = x^7 + 3x^6 + 3x^5 + x^4 - x^3 - 3x^2 - 3x - 1 \in \mathbb{Z}_6[x]$ . Compute the set of all roots of  $R_0(P)$  and then compute the prime factorization of  $P$ .

**Lagrange interpolation** One particularly useful property of polynomials is that a polynomial of degree  $m$  is completely determined on  $m + 1$  evaluation points, which implies that we can uniquely derive a polynomial of degree  $m$  from a set  $S$ :

$$S = \{(x_0, y_0), (x_1, y_1), \dots, (x_m, y_m) \mid x_i \neq x_j \text{ for all indices } i \text{ and } j\} \quad (3.30)$$

Polynomials therefore have the property that  $m + 1$  pairs of points  $(x_i, y_i)$  for  $x_i \neq x_j$  are enough to determine the set of pairs  $(x, P(x))$  for all  $x \in R$ . This “few too many” property of polynomials is used in many places, like for example in erasure codes. It is also of importance in snarks and we therefore need to understand a method to actually compute a polynomial from a set of points.

If the coefficients of the polynomial we want to find have a notion of multiplicative inverse, it is always possible to find such a polynomial using a method called **Lagrange interpolation**, which works as follows: Given a set like 3.30, a polynomial  $P$  of degree  $m$  with  $P(x_i) = y_i$  for all pairs  $(x_i, y_i)$  from  $S$  is given by the following algorithm:

*Example 27.* Let us consider the set  $S = \{(0, 4), (-2, 1), (2, 3)\}$ . Our task is to compute a polynomial of degree 2 in  $\mathbb{Q}[x]$  with coefficients from the rational numbers  $\mathbb{Q}$ . Since  $\mathbb{Q}$  has multiplicative inverses, we can use the Lagrange interpolation algorithm from 4, to compute the

check  
algorithm  
floating

**Algorithm 4** Lagrange Interpolation**Require:**  $R$  must have multiplicative inverses**Require:**  $S = \{(x_0, y_0), (x_1, y_1), \dots, (x_m, y_m) \mid x_i, y_i \in R, x_i \neq x_j \text{ for all indices } i \text{ and } j\}$ **procedure** LAGRANGE-INTERPOLATION( $S$ )  **for**  $j \in (0 \dots m)$  **do**

$$l_j(x) \leftarrow \prod_{i=0; i \neq j}^m \frac{x - x_i}{x_j - x_i} = \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_m)}{(x_j - x_m)}$$

**end for**

$$P \leftarrow \sum_{j=0}^m y_j \cdot l_j$$

**return**  $P$ **end procedure****Ensure:**  $P \in R[x]$  with  $\deg(P) = m$ **Ensure:**  $P(x_j) = y_j$  for all pairs  $(x_j, y_j) \in S$ 

polynomial.

$$\begin{aligned} l_0(x) &= \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x + 2}{0 + 2} \cdot \frac{x - 2}{0 - 2} = -\frac{(x + 2)(x - 2)}{4} \\ &= -\frac{1}{4}(x^2 - 4) \\ l_1(x) &= \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 0}{-2 - 0} \cdot \frac{x - 2}{-2 - 2} = \frac{x(x - 2)}{8} \\ &= \frac{1}{8}(x^2 - 2x) \\ l_2(x) &= \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 0}{2 - 0} \cdot \frac{x + 2}{2 + 2} = \frac{x(x + 2)}{8} \\ &= \frac{1}{8}(x^2 + 2x) \\ P(x) &= 4 \cdot \left(-\frac{1}{4}(x^2 - 4)\right) + 1 \cdot \frac{1}{8}(x^2 - 2x) + 3 \cdot \frac{1}{8}(x^2 + 2x) \\ &= -x^2 + 4 + \frac{1}{8}x^2 - \frac{1}{4}x + \frac{3}{8}x^2 + \frac{3}{4}x \\ &= -\frac{1}{2}x^2 + \frac{1}{2}x + 4 \end{aligned}$$

1602 And, indeed, evaluation of  $P$  on the  $x$ -values of  $S$  gives the correct points, since  $P(0) = 4$ ,  
 1603  $P(-2) = 1$  and  $P(2) = 3$ . Sage provides the following function:

```

1604 sage: Qx = QQ['x'] 150
1605 sage: S=[(0,4), (-2,1), (2,3)] 151
1606 sage: Qx.lagrange_polynomial(S) 152
1607 -1/2*x^2 + 1/2*x + 4 153

```

*Example 28.* To give another example more relevant to the topics of this book, let us consider the same set  $S = \{(0, 4), (-2, 1), (2, 3)\}$  as in the previous example. This time, the task is to compute a polynomial  $P \in \mathbb{Z}_5[x]$  from this data. Since we know from example 14 that multiplicative inverses exist in  $\mathbb{Z}_5$ , algorithm 4 applies and we can compute a unique polynomial of degree 2 in  $\mathbb{Z}_5[x]$  from  $S$ . We can use the lookup tables from example 14 for computation in  $\mathbb{Z}_5$

and get the following:

$$\begin{aligned}
 l_0(x) &= \frac{x-x_1}{x_0-x_1} \cdot \frac{x-x_2}{x_0-x_2} = \frac{x+2}{0+2} \cdot \frac{x-2}{0-2} = \frac{(x+2)(x-2)}{-4} = \frac{(x+2)(x+3)}{1} \\
 &= x^2 + 1 \\
 l_1(x) &= \frac{x-x_0}{x_1-x_0} \cdot \frac{x-x_2}{x_1-x_2} = \frac{x-0}{-2-0} \cdot \frac{x-2}{-2-2} = \frac{x}{3} \cdot \frac{x+3}{1} = 2(x^2 + 3x) \\
 &= 2x^2 + x \\
 l_2(x) &= \frac{x-x_0}{x_2-x_0} \cdot \frac{x-x_1}{x_2-x_1} = \frac{x-0}{2-0} \cdot \frac{x+2}{2+2} = \frac{x(x+2)}{3} = 2(x^2 + 2x) \\
 &= 2x^2 + 4x \\
 P(x) &= 4 \cdot (x^2 + 1) + 1 \cdot (2x^2 + x) + 3 \cdot (2x^2 + 4x) \\
 &= 4x^2 + 4 + 2x^2 + x + x^2 + 2x \\
 &= 2x^2 + 3x + 4
 \end{aligned}$$

1608 And, indeed, evaluation of  $P$  on the  $x$ -values of  $S$  gives the correct points, since  $P(0) = 4$ ,  
 1609  $P(-2) = 1$  and  $P(2) = 3$ . We can doublecheck our findings using Sage:

```

1610 sage: F5 = GF(5)                                     154
1611 sage: F5x = F5['x']                                   155
1612 sage: S = [(0, 4), (-2, 1), (2, 3)]                  156
1613 sage: F5x.lagrange_polynomial(S)                      157
1614 2*x^2 + 3*x + 4                                       158

```

1615 *Exercise 29.* Consider modular 5 arithmetic from example 14 and the set  $S = \{(0, 0), (1, 1), (2, 2), (3, 2)\}$ .  
 1616 Find a polynomial  $P \in \mathbb{Z}_5[x]$  such that  $P(x_i) = y_i$  for all  $(x_i, y_i) \in S$ .

1617 *Exercise 30.* Consider the set  $S$  from the previous example. Why is it not possible to apply  
 1618 algorithm 4 to construct a polynomial  $P \in \mathbb{Z}_6[x]$ , such that  $P(x_i) = y_i$  for all  $(x_i, y_i) \in S$ ?

# Chapter 4

## Algebra

In the previous chapter, we gave an introduction to the basic computational tools needed for a pen-and-paper approach to SNARKs and in this chapter we provide a more abstract clarification of relevant mathematical terminology such as **groups**, **rings** and **fields**.

Scientific literature on cryptography frequently contain such terms, and it is necessary to get at least some understanding of these terms to be able to follow the literature.

### 4.1 Commutative Groups

Commutative groups are abstractions that capture the essence of mathematical phenomena, like addition and subtraction, or multiplication and division.

To understand commutative groups, let us think back to when we learned about the addition and subtraction of integers in school. We have learned that, whenever we add two integers, the result is guaranteed to be an integer as well. We have also learned that adding zero to any integer means that “nothing happens”, that is, the result of the addition is the same integer we started with. Furthermore, we have learned that the order in which we add two (or more) integers does not matter, that brackets have no influence on the result of addition, and that, for every integer, there is always another integer (the negative) such that we get zero when we add them together.

These conditions are the defining properties of a commutative group, and mathematicians have realized that the exact same set of rules can be found in very different mathematical structures. It therefore makes sense to abstract from integers and to give a formal definition of what a group should be, detached from any concrete examples. This lets us handle entities of very different mathematical origins in a flexible way, while retaining essential structural aspects of many objects in abstract algebra and beyond.

Distilling these rules to the smallest independent list of properties and making them abstract, we arrive at the following definition of a commutative group:

*Sylvia: I would like to have a separate counter for definitions*

**Definition 4.1.0.1.** A **commutative group**  $(\mathbb{G}, \cdot)$  is a set  $\mathbb{G}$ , together with a **map**  $\cdot : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}$  called the **group law**, that combines two elements of the set  $\mathbb{G}$  into a third one such that the following properties hold:

- **Commutativity:** For all  $g_1, g_2 \in \mathbb{G}$ , the equation  $g_1 \cdot g_2 = g_2 \cdot g_1$  holds.
- **Associativity:** For every  $g_1, g_2, g_3 \in \mathbb{G}$  the equation  $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$  holds.
- **Existence of a neutral element:** There is a  $e \in \mathbb{G}$  for all  $g \in \mathbb{G}$ , such that  $e \cdot g = g$ .

*Sylvia: I would like to have a separate counter for definitions*

- **Existence of an inverse:** For every  $g \in \mathbb{G}$  there is a  $g^{-1} \in \mathbb{G}$ , such that  $g \cdot g^{-1} = e$ .

If  $(\mathbb{G}, \cdot)$  is a group and  $\mathbb{G}' \subset \mathbb{G}$  is a subset of  $\mathbb{G}$ , such that the restriction of the group law  $\cdot : \mathbb{G}' \times \mathbb{G}' \rightarrow \mathbb{G}'$  is a group law on  $\mathbb{G}'$ , then  $(\mathbb{G}', \cdot)$  is called a **subgroup** of  $(\mathbb{G}, \cdot)$ .

Rephrasing the abstract definition in layman's terms, a group is something where we can do computations in a way that resembles the behavior of the addition of integers. Specifically, this means we can combine some element with another element into a new element in a way that is reversible and where the order of combining elements doesn't matter.

*Notation and Symbols 3.* Since we are exclusively concerned with commutative groups in this book, we often just call them groups, keeping the notation of commutativity implicit. Commutative groups are also called **Abelian groups**. A set  $\mathbb{G}$  with a map  $\cdot$  that satisfies all previously mentioned rules, except for the commutativity law is called a non-commutative group.

If there is no risk of ambiguity (about what the group law of that group is), we frequently drop the symbol  $\cdot$  and simply write  $\mathbb{G}$  as notation for the group, keeping the group law implicit. In this case we also say that  $\mathbb{G}$  is of group type, indicating that  $\mathbb{G}$  is not simply a set but a set together with a group law.

For commutative groups  $(\mathbb{G}, \cdot)$ , we sometimes use the so-called **additive notation**  $(\mathbb{G}, +)$ , that is, we write  $+$  instead of  $\cdot$  for the group law,  $0$  for the neutral element and  $-g := g^{-1}$  for the inverse of an element  $g \in \mathbb{G}$ .

As we will see in the following chapters, groups are heavily used in cryptography and in SNARKs. But let us look at some more familiar examples first:

*Example 29 (Integer Addition and Subtraction).* The set  $(\mathbb{Z}, +)$  of integers with integer addition is the archetypical example of a commutative group, where the group law is traditionally written in additive notation 3.

To compare integer addition against the abstract axioms of a commutative group, we first see that integer addition is commutative and associative, since  $a + b = b + a$  as well as  $(a + b) + c = a + (b + c)$  for all integers  $a, b, c \in \mathbb{Z}$ . The neutral element  $e$  is the number  $0$ , since  $a + 0 = a$  for all integers  $a \in \mathbb{Z}$ . Furthermore, the inverse of a number is its negative counterpart, since  $a + (-a) = 0$ , for all  $a \in \mathbb{Z}$ . This implies that integers with addition are indeed a commutative group in the abstract sense.

To give an example of a subgroup for the group of integers, consider the set  $\mathbb{Z}_{\text{even}} := \{\dots, -4, -2, 0, 2, 4, \dots\}$  of even numbers, including  $0$ . We can see that this set is a subgroup of  $(\mathbb{Z}, +)$ , since the sum of two even numbers is always an even number again, since the neutral element  $0$  is a member of  $\mathbb{Z}_{\text{even}}$  and since the negative of an even number is itself an even number.

*Example 30 (The trivial group).* The most basic example of a commutative group is the group with just one element  $\{\bullet\}$  and the group law  $\bullet \cdot \bullet = \bullet$ . We call it the **trivial group**.

The trivial group is a subgroup of any group. To see that let  $(\mathbb{G}, \cdot)$  be a group with neutral element  $e \in \mathbb{G}$ . Then  $e \cdot e = e$  as well as  $e^{-1} = e$  and it follows that the set  $\{e\}$  is a subgroup of  $\mathbb{G}$ . In particular  $\{0\}$  is a subgroup of  $(\mathbb{Z}, +)$ , since  $0 + 0 = 0$ .

*Example 31.* Consider the addition in modulo 6 arithmetics  $(\mathbb{Z}_6, +)$  as defined in in example 9. As we see, the remainder  $0$  is the neutral element in modulo 6 addition and the inverse of a remainder  $r$  is given by  $6 - r$ , because  $r + (6 - r) = 6$ , which is congruent to  $0$ , since  $6 \bmod 6 = 0$ . Moreover,  $r_1 + r_2 = r_2 + r_1$  as well as  $(r_1 + r_2) + r_3 = r_1 + (r_2 + r_3)$  are inherited from integer addition. We therefore see that  $(\mathbb{Z}_6, +)$  is a group.

The previous example of a commutative group is a very important one for this book. Abstracting from this example and considering residue classes  $(\mathbb{Z}_n, +)$  for arbitrary moduli  $n$ , it can be shown that  $(\mathbb{Z}_n, +)$  is a commutative group with the neutral element  $0$  and the additive

inverse  $n - r$  for any element  $r \in \mathbb{Z}_n$ . We call such a group the **remainder class group** of modulus  $n$ .

*Exercise 31.* Consider example 14 again and let  $\mathbb{Z}_5^*$  be the set of all remainder classes from  $\mathbb{Z}_5$  without the class 0. Then  $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ . Show that  $(\mathbb{Z}_5^*, \cdot)$  is a commutative group.

*Exercise 32.* Generalizing the previous exercise, consider the general modulus  $n$ , and let  $\mathbb{Z}_n^*$  be the set of all remainder classes from  $\mathbb{Z}_n$  without the class 0. Then  $\mathbb{Z}_n^* = \{1, 2, \dots, n-1\}$ . Provide a counter-example to show that  $(\mathbb{Z}_n^*, \cdot)$  is not a group in general.

Find a condition such that  $(\mathbb{Z}_n^*, \cdot)$  is a commutative group, compute the neutral element, give a closed form for the inverse of any element and prove the commutative group axioms.

**Finite groups** As we have seen in the previous examples, groups can either contain infinitely many elements (such as integers) or finitely many elements (as for example the remainder class groups  $(\mathbb{Z}_n, +)$ ). To capture this distinction, a group is called a **finite group** if the underlying set of elements is finite. In that case, the number of elements of that group is called its **order**.

*Notation and Symbols 4.* Let  $\mathbb{G}$  be a finite group. We write  $\text{ord}(\mathbb{G})$  or  $|\mathbb{G}|$  for the order of  $\mathbb{G}$ .

*Example 32.* Consider the remainder class groups  $(\mathbb{Z}_6, +)$  from example 9, the group  $(\mathbb{Z}_5, +)$  from example 14, and the group  $(\mathbb{Z}_5^*, \cdot)$  from exercise 31. We can easily see that the order of  $(\mathbb{Z}_6, +)$  is 6, the order of  $(\mathbb{Z}_5, +)$  is 5 and the order of  $(\mathbb{Z}_5^*, \cdot)$  is 4.

*Exercise 33.* Let  $n \in \mathbb{N}$  with  $n \geq 2$  be some modulus. What is the order of the remainder class group  $(\mathbb{Z}_n, +)$ .

**Generators** The set of elements of a group can be complicated and it is not always obvious how to actually compute elements of a given group. From a practical point of view it is therefore desirable, if a group has a small subset of elements, such that all other elements can be generated by applying the group law repeatedly to the elements of that subset or their inverses only. Sets with these properties are called **generator sets**.

Of course, every group  $\mathbb{G}$  has a trivial set of generators, when we just consider every element of the group to be in the generator set. The more interesting question is to find smallest possible sets of generators for a given group. Of particular interest in this regard are groups that have a generator set that contains a single element only. In this case, there exists a (not necessarily unique) element  $g \in \mathbb{G}$  such that every other element from  $\mathbb{G}$  can be computed by the repeated combination of  $g$  and its inverse  $g^{-1}$  only. Groups with single, not necessarily unique, generators are called **cyclic groups** and any element  $g \in \mathbb{G}$  that is able to generate  $\mathbb{G}$  is called a **generator**.

*Example 33.* The most basic example of a cyclic group is the group of integers  $(\mathbb{Z}, +)$  with integer addition. In this case, the number 1 is a generator of  $\mathbb{Z}$ , since every integer can be obtained by repeatedly adding either 1 or its inverse  $-1$  to itself. For example  $-4$  is generated by 1, since  $-4 = -1 + (-1) + (-1) + (-1)$ . Another generator of  $\mathbb{Z}$  is the number  $-1$ .

*Example 34.* Consider the group  $(\mathbb{Z}_5^*, \cdot)$  from exercise 31. Since  $2^1 = 2$ ,  $2^2 = 4$ ,  $2^3 = 3$  and  $2^4 = 1$ , the element 2 is a generator of  $(\mathbb{Z}_5^*, \cdot)$ . Moreover since  $3^1 = 3$ ,  $3^2 = 4$ ,  $3^3 = 2$  and  $3^4 = 1$ , the element 3 is another generator of  $(\mathbb{Z}_5^*, \cdot)$ . Cyclic groups can therefore have more than one generator. However since  $4^1 = 4$ ,  $4^2 = 1$ ,  $4^3 = 4$  and in general  $4^k = 4$  for  $k$  odd and  $4^k = 1$  for  $k$  even the element 4 is not a generator of  $(\mathbb{Z}_5^*, \cdot)$ . It follows that in general not every element of a finite cyclic group is a generator.

*Example 35.* Consider a modulus  $n$  and the remainder class groups  $(\mathbb{Z}_n, +)$  from exercise 33. These groups are cyclic, with generator 1, since every other element of that group can be constructed by repeatedly adding the remainder class 1 to itself. Since  $\mathbb{Z}_n$  is also finite, we know that  $(\mathbb{Z}_n, +)$  is a finite cyclic group of order  $n$ .

*Exercise 34.* Consider the group  $(\mathbb{Z}_6, +)$  of modular 6 addition from example 9. Show that  $5 \in \mathbb{Z}_6$  is a generator and then show that  $2 \in \mathbb{Z}_6$  is not a generator.

*Exercise 35.* Let  $p \in \mathbb{P}$  be prime number and  $(\mathbb{Z}_p^*, \cdot)$  the finite group from exercise 32. Show that  $(\mathbb{Z}_p^*, \cdot)$  is cyclic.

**The exponential map** Observe that, when  $\mathbb{G}$  is a cyclic group of order  $n$  and  $g \in \mathbb{G}$  is a generator of  $\mathbb{G}$ , then there is the following map with respect to the generator  $g$ :

$$g^{(\cdot)} : \mathbb{Z}_n \rightarrow \mathbb{G} \quad x \mapsto g^x \quad (4.1)$$

In the map above,  $g^x$  means “multiply  $g$   $x$ -times by itself” and  $g^0 = e_{\mathbb{G}}$ . This map, called the **exponential map**, has the remarkable property that it maps the additive group law of the remainder class group  $(\mathbb{Z}_n, +)$  in a one-to-one correspondence to the group law of  $\mathbb{G}$ .

To see this, first observe that, since  $g^0 := e_{\mathbb{G}}$  by definition, the neutral element of  $\mathbb{Z}_n$  is mapped to the neutral element of  $\mathbb{G}$ , and, since  $g^{x+y} = g^x \cdot g^y$ , the map respects the group law.

Because the exponential map respects the group law, it doesn’t matter if we do our computation in  $\mathbb{Z}_n$  before we write the result into the exponent of  $g$  or afterwards: the result will be the same in both cases. This is usually referred to as doing computations “in the exponent”. In cryptography in general, and in SNARK development in particular, we often perform computations “in the exponent” of a generator.

*Example 36.* Consider the multiplicative group  $(\mathbb{Z}_5^*, \cdot)$  from exercise 31. We know from 35 that  $\mathbb{Z}_5^*$  is a cyclic group of order 4, and that the element  $3 \in \mathbb{Z}_5^*$  is a generator. We then know that the following map respects the group law of addition in  $\mathbb{Z}_4$  and the group law of multiplication in  $\mathbb{Z}_5^*$ :

$$3^{(\cdot)} : \mathbb{Z}_4 \rightarrow \mathbb{Z}_5^*, \quad x \mapsto 3^x$$

To do an example computation “in the exponent” of 3, let’s perform the calculation  $1 + 3 + 2$  in the exponent of the generator 3:

$$\begin{aligned} 3^{1+3+2} &= 3^2 \\ &= 4 \end{aligned}$$

What we did is, we first performed the computation  $1 + 3 + 2 = 1$  in the remainder class group  $(\mathbb{Z}_4, +)$  and then applied the exponential map  $3^{(\cdot)}$  to the result.

However since the exponential map 4.1 “respects the group law” we also could map each summand into  $(\mathbb{F}_5^*, \cdot)$  first and then apply the group law of  $(\mathbb{F}_5^*, \cdot)$ . The result is guaranteed to be the same:

$$\begin{aligned} 3^1 \cdot 3^3 \cdot 3^2 &= 3 \cdot 2 \cdot 4 \\ &= 1 \cdot 4 \\ &= 4 \end{aligned}$$



Since the exponential map is a one-to-one correspondence that respects the group law, it can be shown that this map has an inverse with respect to the base  $g$ , called the **base  $g$  discrete logarithm map**:

$$\log_g(\cdot) : \mathbb{G} \rightarrow \mathbb{Z}_n \quad x \mapsto \log_g(x) \quad (4.2)$$

Discrete logarithms are highly important in cryptography, because there are finite cyclic groups where the exponential map and its inverse, the discrete logarithm map, are believed to be one-way functions, which informally means that computing the exponential map is fast, while computing the logarithm map is slow (We will look into a more precise definition in 4.1.1).

*Example 37.* Consider the exponential map  $3^{(\cdot)}$  from example 36. Its inverse is the discrete logarithm to the base 3 and it is given by the map

$$\log_3(\cdot) : \mathbb{Z}_5^* \rightarrow \mathbb{Z}_4 \quad x \mapsto \log_3(x)$$

In contrast to the exponential map  $3^{(\cdot)}$ , we have no way to actually compute this map, other than by trying all elements of the group until we find the correct one. For example in order to compute  $\log_3(4)$ , we have to find some  $x \in \mathbb{Z}_4$ , such that  $3^x = 4$  and all we can do is repeatedly insert elements  $x$  into the exponent of 3 until the result is 4. To do this let's write down all the images of  $3^{(\cdot)}$ :

$$3^0 = 1, \quad 3^1 = 3, \quad 3^2 = 4, \quad 3^3 = 2$$

Since the discrete logarithm  $\log_3(\cdot)$  is defined as the inverse to this function, we can use those images to compute the discrete logarithm:

$$\log_3(1) = 0, \quad \log_3(2) = 3, \quad \log_3(3) = 1, \quad \log_3(4) = 2$$

Note that this computation was only possible, because we were able to write down all images of the exponential map. However, in real world applications the groups in consideration are too large to write down the images of the exponential map.

**Factor Groups** As we know from the fundamental theorem of arithmetics 3.6, every natural number  $n$  is a product of factors, the most basic of which are prime numbers. This reflects into subgroups of a finite cyclic group in an interesting way: If  $\mathbb{G}$ , is a finite cyclic group of order  $n$ , then every subgroup  $\mathbb{G}'$  of  $\mathbb{G}$ , is finite and cyclic and the order of  $\mathbb{G}'$ , is a factor of  $n$ . Moreover for each factor  $k$  of  $n$ ,  $\mathbb{G}$  has exactly one subgroup of order  $k$ . This is known as the **fundamental theorem of finite cyclic groups**.

*Notation and Symbols 5.* If  $\mathbb{G}$  is a finite cyclic group of order  $n$  and  $k$  is a factor of  $n$ , then we write  $\mathbb{G}[k]$  for the unique finite cyclic group, which is the order  $k$  subgroup of  $\mathbb{G}$  and call it a **factor group** of  $\mathbb{G}$ .

One particular interesting situation occurs if the order of a given finite cyclic group is a prime number. As we know from the fundamental theorem of arithmetics 3.6, prime numbers have only two factors, given by the number 1 and the prime number itself. It then follows from the fundamental theorem of finite cyclic groups 4.1, that those groups have no subgroups other than the trivial group 30 and the group itself.

Cryptographic protocols often assume the existence of finite cyclic groups of prime order but sometimes real world implementations of those protocols are not defined on prime order groups, but on groups where the order consist of a (usually large) prime number that has small cofactors 1. In this case a method called **cofactor clearing** has to be applied to ensure that the computations are not done in the group itself but in its (large) prime order subgroup.

To understand cofactor clearing in detail, let  $\mathbb{G}$  be a finite cyclic group of order  $n$  and let  $k$  be a factor of  $n$  with associated factor group  $\mathbb{G}[k]$ . We can project any element  $g \in \mathbb{G}[k]$  onto the neutral element  $e$  of  $\mathbb{G}$  by multiplying  $g$   $k$ -times with itself:

$$g^k = e \quad (4.3)$$

From this follows that if  $c := n \operatorname{div} k$  is the cofactor 1 of  $k$  in  $n$  then any element from the full group  $g \in \mathbb{G}$  can be projected into the factor group  $\mathbb{G}[k]$  by multiplying  $g$   $c$ -times with itself. This defines the following map, which is often called **cofactor clearing** in the cryptographic literature:

$$(\cdot)^c : \mathbb{G} \rightarrow \mathbb{G}[k] : g \mapsto g^c \quad (4.4)$$

*Example 38.* Consider the finite cyclic group  $(\mathbb{Z}_5^*, \cdot)$  from example 34. Since the order of  $\mathbb{Z}_5^*$  is 4 and 4 has the factors 1, 2 and 4, it follows from the fundamental theorem of finite cyclic groups, that  $\mathbb{Z}_5^*$  has 3 unique subgroups. In fact the unique subgroup  $\mathbb{Z}_5^*[1]$  of order 1 is given by the trivial group  $\{1\}$  that contains only the multiplicative neutral element 1 and the unique subgroup  $\mathbb{Z}_5^*[4]$  of order 4 is  $\mathbb{Z}_5^*$  itself, since by definition every group is trivially a subgroup of itself. The unique subgroup  $\mathbb{Z}_5^*[2]$  of order 2 is more interesting and is given by the set  $\mathbb{Z}_5^*[2] = \{1, 4\}$ .

Since  $\mathbb{Z}_5^*$  is not a prime order group and since the only prime factor of 4 is 2, the "large" prime order subgroup of  $\mathbb{Z}_5^*$  is  $\mathbb{Z}_5^*[2]$ . Moreover since the cofactor of 2 in 4 is also 2, we have the cofactor clearing map  $(\cdot)^2 : \mathbb{Z}_5^* \rightarrow \mathbb{Z}_5^*[2]$  and indeed applying this map to all elements from  $\mathbb{Z}_5^*$  we see that it maps onto the elements of  $\mathbb{Z}_5^*[2]$  only:

$$1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 4, \quad 4^2 = 1$$

We can therefore use this map to "clear the cofactor" of any element from  $\mathbb{Z}_5^*$  which means that the element is projected into the "large" prime order subgroup  $\mathbb{Z}_5^*[2]$ .

*Exercise 36.* Consider the previous example 38 and show that  $\mathbb{Z}_5^*[2]$  is a commutative group.

*Exercise 37.* Consider the finite cyclic group  $(\mathbb{Z}_6, +)$  of modular 6 addition from example 34. Describe all subgroups of  $(\mathbb{Z}_6, +)$ . Identify the large prime order subgroup of  $\mathbb{Z}_6$ , define its cofactor clearing map and apply that map to all elements of  $\mathbb{Z}_6$ .

*Exercise 38.* Let  $(\mathbb{Z}_p^*, \cdot)$  be the cyclic group from exercise 35. Show that for  $p \geq 5$ , not every element  $x \in \mathbb{F}_p^*$  is a generator of  $\mathbb{F}_p^*$ .

**Pairings** Of particular importance for the development of SNARKs are so-called pairing maps on commutative groups. To see the definition, let  $\mathbb{G}_1$ ,  $\mathbb{G}_2$  and  $\mathbb{G}_3$  be three commutative groups. Then a **pairing map** is a function

$$e(\cdot, \cdot) : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3 \quad (4.5)$$

This function takes pairs  $(g_1, g_2)$  of elements from  $\mathbb{G}_1$  and  $\mathbb{G}_2$ , and maps them to elements from  $\mathbb{G}_3$ , such that the **bilinearity** property holds, which means that for all  $g_1, g'_1 \in \mathbb{G}_1$  and  $g_2, g'_2 \in \mathbb{G}_2$  the following two identities are satisfied:

$$e(g_1 \cdot g'_1, g_2) = e(g_1, g_2) \cdot e(g'_1, g_2) \quad \text{and} \quad e(g_1, g_2 \cdot g'_2) = e(g_1, g_2) \cdot e(g_1, g'_2) \quad (4.6)$$

Informally speaking, bilinearity means that it doesn't matter if we first execute the group law on one side and then apply the bilinear map, or if we first apply the bilinear map and then apply the group law in  $\mathbb{G}_3$ .

A pairing map is called **non-degenerate** if, whenever the result of the pairing is the neutral element in  $\mathbb{G}_3$ , one of the input values is the neutral element of  $\mathbb{G}_1$  or  $\mathbb{G}_2$ . To be more precise,  $e(g_1, g_2) = e_{\mathbb{G}_3}$  implies  $g_1 = e_{\mathbb{G}_1}$  or  $g_2 = e_{\mathbb{G}_2}$ .

*Example 39.* One of the most basic examples of a non-degenerate pairing involves  $\mathbb{G}_1, \mathbb{G}_2$  and  $\mathbb{G}_3$  all to be the group of integers with addition  $(\mathbb{Z}, +)$ . Then the following map defines a non-degenerate pairing:

$$e(\cdot, \cdot) : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \quad (a, b) \mapsto a \cdot b$$

Note that bilinearity follows from the distributive law of integers, since for  $a, b, c \in \mathbb{Z}$ , we have  $e(a + b, c) = (a + b) \cdot c = a \cdot c + b \cdot c = e(a, c) + e(b, c)$  and the same reasoning is true for the second argument.

To see that  $e(\cdot, \cdot)$  is non-degenerate, assume that  $e(a, b) = 0$ . Then  $a \cdot b = 0$  implies that  $a$  or  $b$  must be zero.

*Exercise 39* (Arithmetic laws for pairing maps). Let  $\mathbb{G}_1, \mathbb{G}_2$  as well as  $\mathbb{G}_3$  be finite cyclic groups of the same order  $n$  and let  $e(\cdot, \cdot) : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$  be a pairing map. Show that for given  $g_1 \in \mathbb{G}_1$  and  $g_2 \in \mathbb{G}_2$  and all  $a, b \in \mathbb{Z}_n$  the following identity holds:

$$e(g_1^a, g_2^b) = e(g_1, g_2)^{a \cdot b} \quad (4.7)$$

*Exercise 40.* Consider the remainder class groups  $(\mathbb{Z}_n, +)$  from example 33 for some modulus  $n$ . Show that the map

$$e(\cdot, \cdot) : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n \quad (a, b) \mapsto a \cdot b$$

is a pairing map. Why is the pairing not non-degenerate in general and what condition must be imposed on  $n$ , such that the pairing will be non-degenerate?

### 4.1.1 Cryptographic Groups

In this section, we will look at families of groups that are believed to satisfy certain **computational hardness assumptions**, namely that a particular problem cannot be solved efficiently (where efficiently typically means “in polynomial time of a given security parameter”) in the groups under consideration.

*Example 40.* To highlight the concept of the computational hardness assumption, consider the group of integers  $\mathbb{Z}$  from example 3.5. One of the best known and most researched examples of computational hardness is the assumption that the factorization of integers into prime numbers cannot be solved by any algorithm in polynomial time with respect to the bit-length of the integer.

To be more precise, the computational hardness assumption of integer factorization assumes that, given any integer  $z \in \mathbb{Z}$  with bit-length  $b$ , there is no integer  $k$  and no algorithm with the runtime complexity of  $\mathcal{O}(b^k)$  that is able to find the prime numbers  $p_1, p_2, \dots, p_j \in \mathbb{P}$ , such that  $z = p_1 \cdot p_2 \cdot \dots \cdot p_j$ .

This hardness assumption was proven to be false, since Shor’s (?) algorithm shows that integer factorization is at least efficiently possible on a quantum computer, since the runtime complexity of this algorithm is  $\mathcal{O}(b^3)$ . However, no such algorithm is known on a classical computer.

In the realm of classical computers, however, we still have to call the non-existence of such an algorithm an “assumption” because, to date, there is no proof that it is actually impossible to find one. The problem is that it is hard to reason about algorithms that we don’t know.

So, despite the fact that there is currently no known algorithm that can factor integers efficiently on a classical computer, we cannot exclude that such an algorithm might exist in principle, and that someone eventually will discover it in the future.

However, what still makes the assumption plausible, despite the absence of any actual proof, is the fact that, after decades of extensive search, still no such algorithm has been found.

check  
reference

runtime  
complex-  
ity

add refer-  
ence

S: what  
does “effi-  
ciently”  
mean  
here?

In what follows, we will describe a few **computational hardness assumptions** that arise in the context of groups in cryptography, because we will refer to them throughout the book.

computational  
hardness  
assump-  
tions

**The discrete logarithm assumption** The so-called discrete logarithm problem is one of the most fundamental assumptions in cryptography. To define it, let  $\mathbb{G}$  be a finite cyclic group of order  $r$  and let  $g$  be a generator of  $\mathbb{G}$ . We know from 4.1 that there is an exponential map  $g^{(\cdot)} : \mathbb{Z}_r \rightarrow \mathbb{G} : x \mapsto g^x$  that maps the residue classes from modulo  $r$  arithmetic onto the group in a 1 : 1 correspondence. The **discrete logarithm problem** is the task of finding inverses to this map, that is, to find a solution  $x \in \mathbb{Z}_r$  to the following equation for some given  $h \in \mathbb{G}$ :

check  
reference

$$h = g^x \quad (4.8)$$

In other words, the **discrete logarithm assumption (DL-A)** is the assumption that there exists no algorithm with polynomial running time in the security parameter  $\log_2(r)$ , that is able to compute some  $x$  if only  $h$ ,  $g$  and  $g^x$  are given in  $\mathbb{G}$ . If this is the case for  $\mathbb{G}$ , we call  $\mathbb{G}$  a **DL-A group**.

Rephrasing the previous definition, DL-A groups are believed to have the property that it is infeasible to compute some number  $x$  that solves the equation  $h = g^x$  for a given  $h$  and  $g$ , assuming that the size of the group  $r$  is large enough.

*Example 41* (Public key cryptography). One the most basic examples of an application for DL-A groups is in public key cryptography, where the parties publicly agree on some pair  $(\mathbb{G}, g)$  such that  $\mathbb{G}$  is a finite cyclic group of sufficiently large order  $r$ , where  $\mathbb{G}$  is believed to be a DL-A group, and  $g$  is a generator of  $\mathbb{G}$ .

In this setting, a secret key is some number  $sk \in \mathbb{Z}_r$  and the associated public key  $pk$  is the group element  $pk = g^{sk}$ . Since discrete logarithms are assumed to be hard, it is infeasible for an attacker to compute the secret key from the public key, since it is believed to be hard to find solutions  $x$  to the following equation:

$$pk = g^x \quad (4.9)$$

As the previous example shows, identifying DL-A groups is an important practical problem. Unfortunately, it is easy to see that it does not make sense to assume the hardness of the discrete logarithm problem in all finite cyclic groups: Counterexamples are common and easy to construct.

*Example 42* (Modular arithmetics for Fermat's primes). It is widely believed that the discrete logarithm problem is hard in multiplicative groups  $\mathbb{Z}_p^*$  of prime number modular arithmetics. However, this is not true in general. To see that, consider any so-called Fermat's prime, which is a prime number  $p \in \mathbb{P}$ , such that  $p = 2^n + 1$  for some number  $n$ .

We know from exercise 32 that in this case  $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$  is a group with respect to integer multiplication in modular  $p$  arithmetics and since  $p = 2^n + 1$ , the order of  $\mathbb{Z}_p^*$  is  $2^n$ , which implies that the associated security parameter is given by  $\log_2(2^n) = n$ .

check  
reference

We show that, in this case,  $\mathbb{Z}_p^*$  is not a DL-A group, by constructing an algorithm, which is able to compute some  $x \in \mathbb{Z}_{2^n}$  for any given generator  $g$  and arbitrary element  $h$  of  $\mathbb{F}_p^*$ , such that equation 4.10 holds, and the runtime complexity of the constructed algorithm is  $\mathcal{O}(n^2)$ , which is quadratic in the security parameter  $n = \log_2(2^n)$ .

$$h = g^x \quad (4.10)$$

To define such an algorithm, let us assume that the generator  $g$  is a public constant and that a group element  $h$  is given. Our task is to compute  $x$  efficiently.

The first thing to note is that, since  $x$  is a number in modular  $2^n$  arithmetic, we can write the binary representation of  $x$  as in 4.11, with binary coefficients  $c_j \in \{0, 1\}$ . In particular,  $x$  is an  $n$ -bit number if interpreted as an integer.

$$x = c_0 \cdot 2^0 + c_1 \cdot 2^1 + \cdots + c_n \cdot 2^n \quad (4.11)$$

We then use this representation to construct an algorithm that computes the bits  $c_j$  one after another, starting at  $c_0$ . To see how this can be achieved, observe that we can determine  $c_0$  by raising the input  $h$  to the power of  $2^{n-1}$  in  $\mathbb{F}_p^*$ . We use the exponential laws and compute as follows:

$$\begin{aligned} h^{2^{n-1}} &= (g^x)^{2^{n-1}} \\ &= \left( g^{c_0 \cdot 2^0 + c_1 \cdot 2^1 + \cdots + c_n \cdot 2^n} \right)^{2^{n-1}} \\ &= g^{c_0 \cdot 2^{n-1}} \cdot g^{c_1 \cdot 2^1 \cdot 2^{n-1}} \cdot g^{c_2 \cdot 2^2 \cdot 2^{n-1}} \cdots g^{c_n \cdot 2^n \cdot 2^{n-1}} \\ &= g^{c_0 2^{n-1}} \cdot g^{c_1 2^0 \cdot 2^n} \cdot g^{c_2 2^1 \cdot 2^n} \cdots g^{c_n 2^{n-1} \cdot 2^n} \end{aligned}$$

Now, since  $g$  is a generator and  $\mathbb{F}_p^*$  is cyclic of order  $2^n$ , we know  $g^{2^n} = 1$  and therefore  $g^{k \cdot 2^n} = 1^k = 1$ . From this, it follows that all but the first factor in the last expression are equal to 1 and we can simplify the expression into the following:

$$h^{2^{n-1}} = g^{c_0 2^{n-1}} \quad (4.12)$$

Now, in case  $c_0 = 0$ , we get  $h^{2^{n-1}} = g^0 = 1$ . In case  $c_0 = 1$ , we get  $h^{2^{n-1}} = g^{2^{n-1}} \neq 1$  (To see that  $g^{2^{n-1}} \neq 1$ , recall that  $g$  is a generator of  $\mathbb{F}_p^*$  and hence, is  $\mathbb{F}_p^*$  a cyclic group of order  $2^n$ , which implies  $g^y \neq 1$  for all  $y < 2^n$ ).

Raising  $h$  to the power of  $2^{n-1}$  determines  $c_0$ , and we can apply the same reasoning to the coefficient  $c_1$  by raising  $h \cdot g^{-c_0 \cdot 2^0}$  to the power of  $2^{n-2}$ . This approach can then be repeated until all the coefficients  $c_j$  of  $x$  are found.

Assuming that exponentiation in  $\mathbb{F}_p^*$  can be done in logarithmic runtime complexity  $\log(p)$ , it follows that our algorithm has a runtime complexity of  $\mathcal{O}(\log^2(p)) = \mathcal{O}(n^2)$ , since we have to execute  $n$  exponentiations to determine the  $n$  binary coefficients of  $x$ .

From this, it follows that whenever  $p$  is a Fermat's prime, the discrete logarithm assumption does not hold in  $F_p^*$ .

**The decisional Diffie–Hellman assumption** Let  $\mathbb{G}$  be a finite cyclic group of order  $r$  and let  $g$  be a generator of  $\mathbb{G}$ . The decisional Diffie–Hellman assumption stipulates that there is no algorithm that has a polynomial runtime complexity in the security parameter  $s = \log(r)$  that is able to distinguish the so-called DDH- triple  $(g^a, g^b, g^{ab})$  from any triple  $(g^a, g^b, g^c)$  for randomly and independently chosen parameters  $a, b, c \in \mathbb{Z}_r$ . If this is the case for  $\mathbb{G}$ , we call  $\mathbb{G}$  a **DDH-A group**.

DDH-A is a stronger assumption than DL-A, in the sense that the discrete logarithm assumption is necessary for the decisional Diffie–Hellman assumption to hold, but not the other way around.

To see why this is the case, assume that the discrete logarithm assumption does not hold. In that case, given a generator  $g$  and a group element  $h$ , it is easy to compute some residue class  $x \in \mathbb{Z}_p$  with  $h = g^x$ . Then the decisional Diffie–Hellman assumption cannot hold, since given

explain  
last sen-  
tence  
more

some triple  $(g^a, g^b, z)$ , one could efficiently decide whether  $z = g^{ab}$  is true by first computing the discrete logarithm  $b$  of  $g^b$ , then computing  $g^{ab} = (g^a)^b$  and deciding whether or not  $z = g^{ab}$ .

On the other hand, the following example shows that there are groups where the discrete logarithm assumption holds but the decisional Diffie–Hellman assumption does not.

*Example 43* (Efficiently computable pairings). Let  $\mathbb{G}$  be a finite, cyclic group of order  $r$  with generator  $g$ , such that the discrete logarithm assumption holds and there is a pairing map  $e(\cdot, \cdot) : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$  for some target group  $\mathbb{G}_T$  that is computable in polynomial time of the parameter  $\log(r)$ .

In a setting like this, it is easy to show that DDH-A cannot hold, since given some triple  $(g^a, g^b, z)$ , it is possible to decide in polynomial time w.r.t  $\log(r)$  whether  $z = g^{ab}$  or not. To see that, check the following equation:

$$e(g^a, g^b) = e(g, z) \quad (4.13)$$

Since the bilinearity properties of  $e(\cdot, \cdot)$  imply  $e(g^a, g^b) = e(g, g)^{ab} = e(g, g^{ab})$ , and  $e(g, y) = e(g, y')$  implies  $y = y'$  due to the non-degenerate property, the equality means  $z = e^{ab}$ .

It follows that DDH-A is indeed weaker than DL-A, and groups with efficient pairings cannot be DDH-A groups. The following example shows another important class of groups where DDH-A does not hold: multiplicative groups of prime number residue classes.

*Example 44.* Let  $p$  be a prime number and  $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$  the multiplicative group of modular  $p$  arithmetics as in exercise 32. As we have seen in XXX, this group is finite and cyclic of order  $p-1$  and every element  $g \neq 1$  is a generator.

To see that  $\mathbb{F}_p^*$  cannot be a DDH-A group, recall from XXX that the **Legendre symbol**  $\left(\frac{x}{p}\right)$  of any  $x \in \mathbb{F}_p^*$  is efficiently computable by **Euler’s formular**. But the Legendre symbol of  $g^a$  reveals whether  $a$  is even or odd. Given  $g^a, g^b$  and  $g^{ab}$ , one can thus efficiently compute and compare the least significant bit of  $a, b$  and  $ab$ , respectively, which provides a probabilistic method to distinguish  $g^{ab}$  from a random group element  $g^c$ .

**The computational Diffie–Hellman assumption** Let  $\mathbb{G}$  be a finite cyclic group of order  $r$  and let  $g$  be a generator of  $\mathbb{G}$ . The computational Diffie–Hellman assumption stipulates that, given randomly and independently chosen residue classes  $a, b \in \mathbb{Z}_r$ , it is not possible to compute  $g^{ab}$  if only  $g, g^a$  and  $g^b$  (but not  $a$  and  $b$ ) are known. If this is the case for  $\mathbb{G}$ , we call  $\mathbb{G}$  a CDH-A group.

In general, we don’t know if CDH-A is a stronger assumption then DL-A, or if both assumptions are equivalent. We know that DL-A is necessary for CDH-A, but the other direction is currently not well understood. In particular, there are no groups known where DL-A holds but CDH-A does not hold [?].

To see why the discrete logarithm assumption is necessary, assume that it does not hold. So, given a generator  $g$  and a group element  $h$ , it is easy to compute some residue class  $x \in \mathbb{Z}_p$  with  $h = g^x$ . In that case, the computational Diffie–Hellman assumption cannot hold, since, given  $g, g^a$  and  $g^b$ , one can efficiently compute  $b$  and hence is able to compute  $g^{ab} = (g^a)^b$  from this data.

The computational Diffie–Hellman assumption is a weaker assumption than the decisional Diffie–Hellman assumption, which means that there are groups where CDH-A holds and DDH-A does not hold, while there cannot be groups such that DDH-A holds but CDH-A does not hold. To see that, assume that it is efficiently possible to compute  $g^{ab}$  from  $g, g^a$  and  $g^b$ . Then, given  $(g^a, g^b, z)$  it is easy to decide if  $z = g^{ab}$  holds or not.

“equation”?

check  
reference

what’s the  
difference  
between  
 $\mathbb{F}_p^*$  and  
 $\mathbb{Z}_p^*$ ?

Legendre  
symbol

Euler’s  
formular

These  
are only  
explained  
later in  
the text,  
‘4.33’



Several variations and special cases of the CDH-A exist. For example, the **square computational Diffie–Hellman assumption** assumes that, given  $g$  and  $g^x$ , it is computationally hard to compute  $g^{x^2}$ . The **inverse computational Diffie–Hellman assumption** assumes that, given  $g$  and  $g^x$ , it is computationally hard to compute  $g^{x^{-1}}$ .

## Cofactor Clearing

### 4.1.2 Hashing to Groups

**Hash functions** Generally speaking, a hash function is any function that can be used to map data of arbitrary size to fixed-size values. Since binary strings of arbitrary length are a general way to represent arbitrary data, we can understand a general **hash function** as the following map where  $\{0,1\}^*$  represents the set of all binary strings of arbitrary but finite length and  $\{0,1\}^k$  represents the set of all binary strings that have a length of exactly  $k$  bits:

$$H : \{0,1\}^* \rightarrow \{0,1\}^k \quad (4.14)$$

In our definition, a hash function maps binary strings of arbitrary size onto binary strings of size exactly  $k$ . The **images** of  $H$ , that is, the values returned by the hash function  $H$ , are called **hash values**, **digests**, or simply **hashes**.

A hash function must be deterministic, that is, when we insert the same input  $x$  into  $H$ , the image  $H(x)$  must always be the same. In addition, a hash function should be as uniform as possible, which means that it should map input values as evenly as possible over its output range. In mathematical terms, every string of length  $k$  from  $\{0,1\}^k$  should be generated with roughly the same probability.

*Example 45 ( $k$ -truncation hash).* One of the most basic hash functions  $H_k : \{0,1\}^* \rightarrow \{0,1\}^k$  is given by simply truncating every binary string  $s$  of size  $s.len() > k$  to a string of size  $k$  and by filling any string  $s'$  of size  $s'.len() < k$  with zeros. To make this hash function deterministic, we define that both truncation and filling should happen “on the left”.

For example, if  $k = 3$ ,  $x_1 = (0000101011101010011101010101)$  and  $x_2 = 1$ , then  $H(x_1) = (101)$  and  $H(x_2) = (001)$ . It is easy to see that this hash function is deterministic and uniform.

Of particular interest are so-called **cryptographic** hash functions, which are hash functions that are also **one-way functions**, which essentially means that, given a string  $y$  from  $\{0,1\}^k$  it is practically infeasible to find a string  $x \in \{0,1\}^*$  such that  $H(x) = y$  holds. This property is usually called **preimage-resistance**.

In addition, it should be infeasible to find two strings  $x_1, x_2 \in \{0,1\}^*$ , such that  $H(x_1) = H(x_2)$ , which is called **collision resistance**. It is important to note, though, that collisions always exist, since a function  $H : \{0,1\}^* \rightarrow \{0,1\}^k$  inevitably maps infinitely many values onto the same hash. In fact, for any hash function with digests of length  $k$ , finding a preimage to a given digest can always be done using a brute force search in  $2^k$  evaluation steps. It should just be practically impossible to compute those values, and statistically very unlikely to generate two of them by chance.

A third property of a cryptographic hash function is that small changes in the input string, like changing a single bit, should generate hash values that look completely different from each other.

Because cryptographically secure hash functions map tiny changes in input values onto large changes in the output, implementation errors that change the outcome are usually easy to spot by comparing them to expected output values. The definitions of cryptographically secure

are these going to be relevant later? yes, they are used in various snark proof systems

TODO: theorem: every factor of order defines a subgroup...

Is there a term for this property?

hash functions are therefore usually accompanied by some test vectors of common inputs and expected digests. Since the empty string  $''$  is the only string of length 0, a common test vector is the expected digest of the empty string.

*Example 46* ( $k$ -truncation hash). Consider the  $k$ -truncation hash from example 45. Since the empty string has length 0, it follows that the digest of the empty string is string of length  $k$  that only contains 0's:

$$H_k('') = (000 \dots 000) \quad (4.15)$$

It is pretty obvious from the definition of  $H_k$  that this simple hash function is not a cryptographic hash function. In particular, every digest is its own preimage, since  $H_k(y) = y$  for every string of size exactly  $k$ . Finding preimages is therefore easy, so the property of preimage resistance does not hold.

In addition, it is easy to construct collisions as all strings of size  $> k$  that share the same  $k$ -bits “on the right” are mapped to the same hash value, so this function is not collision resistant, either.

Finally, this hash function is not very chaotic, as changing bits that are not part of the  $k$  right-most bits don't change the digest at all.

Computing cryptographically secure hash functions in pen-and-paper style is possible but tedious. Fortunately, Sage can import the **hashlib** library, which is intended to provide a reliable and stable base for writing Python programs that require cryptographic functions. The following examples explain how to use hashlib in Sage.

*Example 47.* An example of a hash function that is generally believed to be a cryptographically secure hash function is the so-called **SHA256** hash, which, in our notation, is a function that maps binary strings of arbitrary length onto binary strings of length 256:

$$SHA256 : \{0, 1\}^* \rightarrow \{0, 1\}^{256} \quad (4.16)$$

To evaluate a proper implementation of the *SHA256* hash function, the digest of the empty string is supposed to be

$$SHA256('') = e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 \quad (4.17)$$

For better human readability, it is common practice to represent the digest of a string not in its binary form, but in a hexadecimal representation. We can use Sage to compute *SHA256* and freely transit between binary, hexadecimal and decimal representations. To do so, we import hashlib's implementation of *SHA256*:

```
sage: import hashlib 159
sage: test = 'e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934 160
ca495991b7852b855'
sage: hasher = hashlib.sha256(b'') 161
sage: str = hasher.hexdigest() 162
sage: type(str) 163
<class 'str'> 164
sage: d = ZZ('0x' + str) # conversion to integer type 165
sage: d.str(16) == str 166
True 167
sage: d.str(16) == test 168
True 169
```



```

2056 sage: d.str(16) 170
2057 e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b8 171
2058 55
2059 sage: d.str(2) 172
2060 11100011101100001100010001000010100110001111110000011100000101 173
2061 0010011010111110111110100110010001001100101101111101110010
2062 01001000010011110101110010000011110010001100100100110111001
2063 00110100110010100100100101011001100100011011011110000101001
2064 01011100001010101
2065 sage: d.str(10) 174
2066 10298733624955409702953521232258132278979990064819803499337939 175
2067 7001115665086549

```

**Hashing to cyclic groups** As we have seen in the previous paragraph, general hash functions map binary strings of arbitrary length onto binary strings of length  $k$ . However, it is desirable in various cryptographic primitives to not simply hash to binary strings of fixed length but to hash into algebraic structures like groups, while keeping (some of) the properties like preimage resistance or collision resistance.

Hash functions like this can be defined for various algebraic structures, but, in a sense, the most fundamental ones are hash functions that map into groups, because they can be easily extended to map into other structures like rings or fields.

To give a more precise definition, let  $\mathbb{G}$  be a group and  $\{0, 1\}^*$  the set of all finite, binary strings, then a **hash-to-group** function is a deterministic map

$$H : \{0, 1\}^* \rightarrow \mathbb{G} \quad (4.18)$$

Common properties of hash functions, like uniformity, are desirable but not always realized in real-world instantiations of hash-to-group functions, so we skip those requirements for now and keep the definition very general.

As the following example shows, hashing to finite cyclic groups can be trivially achieved for the price of some undesirable properties of the hash function:

*Example 48 (Naive cyclic group hash).* Let  $\mathbb{G}$  be a finite cyclic group. If the task is to implement a hash-to-group function, one immediate approach can be based on the observation that binary strings of size  $k$  can be interpreted as integers  $z \in \mathbb{Z}$  in the range  $0 \leq z < 2^k$ .

To be more precise, choose an ordinary hash function  $H : \{0, 1\}^* \rightarrow \{0, 1\}^k$  for some parameter  $k$  and a generator  $g$  of  $\mathbb{G}$ . Then the expression below is a positive integer (where  $H(s)_j$  means the bit at the  $j$ -th position of  $H(s)$ ):

$$z_{H(s)} = H(s)_0 \cdot 2^0 + H(s)_1 \cdot 2^1 + \dots + H(s)_k \cdot 2^k \quad (4.19)$$

A hash-to-group function for the group  $\mathbb{G}$  can then be defined as a concatenation of the exponential map  $g^{(\cdot)}$  of  $g$  with the interpretation of  $H(s)$  as an integer:

$$H_g : \{0, 1\}^* \rightarrow \mathbb{G} : s \mapsto g^{z_{H(s)}} \quad (4.20)$$

Constructing a hash-to-group function like this is easy for cyclic groups, and it might be good enough in certain applications. It is, however, almost never adequate in cryptographic applications, as discrete log relations might be constructible between two given hash values  $H_g(s)$  and  $H_g(t)$ .

a few examples?

To see that, assume that  $\mathbb{G}$  is of order  $r$  and that  $z_{H(s)}$  has a multiplicative inverse in modular  $r$  arithmetics. In that case, we can compute  $x = z_{H(t)} \cdot z_{H(s)}^{-1}$  in  $\mathbb{Z}_r$  and find a discrete log relation between the group hash values, that is, find some  $x$  with  $H_g(t) = (H_g(s))^x$ :

$$\begin{aligned} H_g(t) &= (H_g(s))^x && \Leftrightarrow \\ g^{z_{H(t)}} &= g^{z_{H(s)} \cdot x} && \Leftrightarrow \\ g^{z_{H(t)}} &= g^{z_{H(t)}} \end{aligned}$$

Therefore applications where discrete log relations between hash values are undesirable need different approaches. Many of these approaches start with a way to hash into the set  $\mathbb{Z}_r$  of modular  $r$  arithmetics.

**Hashing to modular arithmetics** One of the most widely used applications of hash-into-group functions are hash functions that map into the set  $\mathbb{Z}_r$  of modular  $r$  arithmetics for some modulus  $r$ . Different approaches to construct such a function are known, but probably the most widely used ones are based on the insight that the images of arbitrary hash functions can be interpreted as binary representations of integers, as explained in example 48.

It follows from this interpretation that one simple method of hashing into  $\mathbb{Z}_r$  is constructed by observing that if  $r$  is a modulus with a bit-length of  $k = r.\text{nbits}()$ , then every binary string  $(b_0, b_1, \dots, b_{k-2})$  of length  $k - 1$  defines an integer  $z$  in the range  $0 \leq z < 2^{k-1} \leq r$ , by defining  $z$ :

$$z = b_0 \cdot 2^0 + b_1 \cdot 2^1 + \dots + b_{k-2} \cdot 2^{k-2} \quad (4.21)$$

Now, since  $z < r$ , we know that  $z$  is guaranteed to be in the set  $\{0, 1, \dots, r-1\}$ , and hence it can be interpreted as an element of  $\mathbb{Z}_r$ . From this it follows that if  $H : \{0, 1\}^* \rightarrow \{0, 1\}^{k-1}$  is a hash function, then a hash-to-group function can be constructed as follows (where  $H(s)_j$  means the  $j$ -th bit of the image binary string  $H(s)$  of the original binary hash function):

$$H_{r.\text{nbits}()-1} : \{0, 1\}^* \rightarrow \mathbb{Z}_r : s \mapsto H(s)_0 \cdot 2^0 + H(s)_1 \cdot 2^1 + \dots + H(s)_{k-2} \cdot 2^{k-2} \quad (4.22)$$

A drawback of this hash function is that the distribution of the hash values in  $\mathbb{Z}_r$  is not necessarily uniform. In fact, if  $r - 2^{k-1} \neq 0$ , then by design  $H_{r.\text{nbits}()-1}$  will never hash onto values  $z \geq 2^{k-1}$ . Good moduli  $r$  are therefore as close to  $2^{k-1}$  as possible, while less good moduli are closer to  $2^k$ . In the worst case, when  $r = 2^k - 1$ , it misses  $2^{k-1} - 1$ , that is, almost half of all elements, from  $\mathbb{Z}_r$ .

An advantage of this approach is that properties like preimage resistance or collision resistance of the original hash function  $H(\cdot)$  are preserved.

*Example 49.* To give an implementation of the  $H_{r.\text{nbits}()-1}$  hash function, we use a 5-bit truncation of the *SHA256* hash from example 47 and define a hash into  $\mathbb{Z}_{16}$  as follows:

$$H_{16.\text{nbits}()-1} : \{0, 1\}^* \rightarrow \mathbb{Z}_{16} : s \mapsto \text{SHA256}(s)_0 \cdot 2^0 + \text{SHA256}(s)_1 \cdot 2^1 + \dots + \text{SHA256}(s)_4 \cdot 2^4$$

Since  $k = 16.\text{nbits}() = 5$  and  $16 - 2^{k-1} = 0$ , this hash maps uniformly onto  $\mathbb{Z}_{16}$ . We can invoke Sage to implement it:

```

2119 sage: import hashlib                                176
2120 sage: def Hash5(x):                                177
2121     ....:     hasher = hashlib.sha256(x)             178
2122     ....:     digest = hasher.hexdigest()            179
2123     ....:     d = ZZ(digest, base=16)                180
2124     ....:     d = d.str(2)[-4:]                      181
2125     ....:     return ZZ(d, base=2)                  182

```

check  
reference

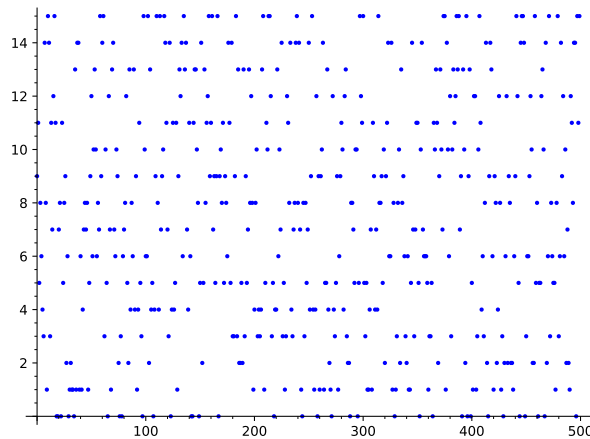
TODO:  
DOUBLE  
CHECK  
THIS  
REA-  
SONING.

2126 `sage: Hash5(b'')`  
 2127 `5`

183

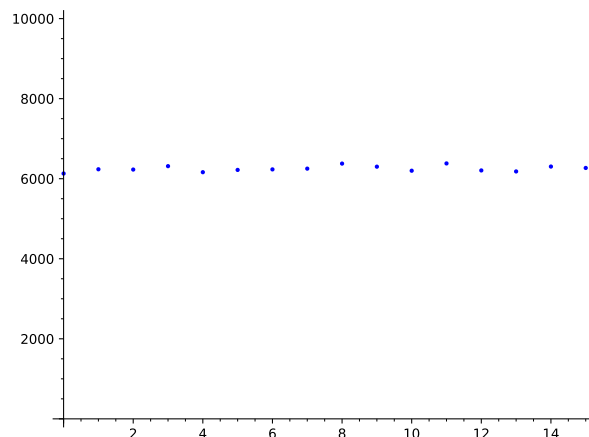
184

2128 We can then use Sage to apply this function to a large set of input values in order to plot a  
 2129 visualization of the distribution over the set  $\{0, \dots, 15\}$ . Executing over 500 input values gives  
 2130 the following plot:



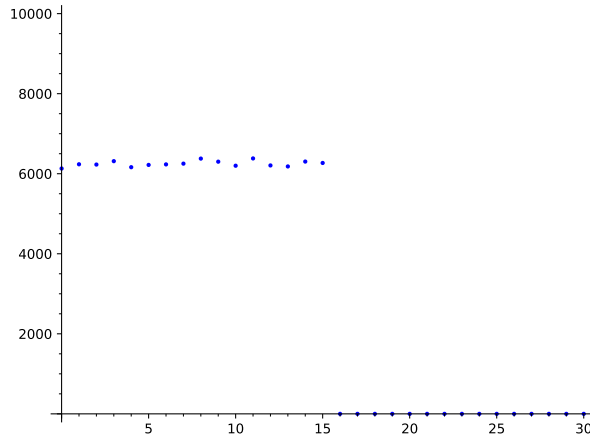
2131

2132 To get an intuition of uniformity, we can count the number of times the hash function  $H_{16.nb\text{its}()-1}$   
 2133 maps onto each number in the set  $\{0, 1, \dots, 15\}$  in a loop of 100000 hashes, and compare that  
 2134 to the ideal uniform distribution, which would map exactly 6250 samples to each element. This  
 2135 gives the following result:



2136

2137 The uniformity of distribution problem becomes apparent if we want to construct a similar hash  
 2138 function for  $\mathbb{Z}_r$  for any  $r$  in the range  $17 \leq r \leq 31$ . In this case, the definition of the hash  
 2139 function is exactly the same as for  $\mathbb{Z}_{16}$ , and hence, the images will not exceed the value 16.  
 2140 So, for example, even in the case of hashing to  $\mathbb{Z}_{31}$ , the hash function never maps to any value  
 2141 larger than 16, leaving almost half of all numbers out of the image range.



Mirco:  
We can  
do better  
than this

The second widely used method of hashing into  $\mathbb{Z}_r$  is constructed by observing the following: If  $r$  is a modulus with a bit-length of  $r.bits() = k_1$  and  $H : \{0, 1\}^* \rightarrow \{0, 1\}^{k_2}$  is a hash function that produces digests of size  $k_2$ , with  $k_2 \geq k_1$ , then a hash-to-group function can be constructed by interpreting the image of  $H$  as a binary representation of an integer and then taking the modulus by  $r$  to map into  $\mathbb{Z}_r$ . This is formalized in the equation below, where  $H(s)_j$  means the  $j$ 'th bit of the image binary string  $H(s)$  of the original binary hash function.

$$H'_{mod_r} : \{0, 1\}^* \rightarrow \mathbb{Z}_r : s \mapsto \left( H(s)_0 \cdot 2^0 + H(s)_1 \cdot 2^1 + \dots + H(s)_{k_2} \cdot 2^{k_2} \right) \bmod n \quad (4.23)$$

A drawback of this hash function is that computing the modulus requires some computational effort. In addition, the distribution of the hash values in  $\mathbb{Z}_r$  might not be even, depending on the difference  $2^{k_2+1} - r$ . An advantage of it is that potential properties of the original hash function  $H(\cdot)$  (like preimage resistance or collision resistance) are preserved, and the distribution can be made almost uniform, with only negligible bias depending on what modulus  $r$  and images size  $k_2$  are chosen.

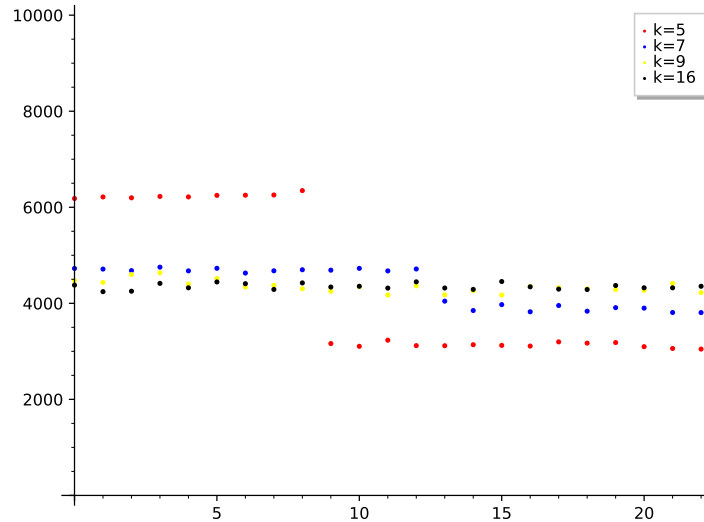
*Example 50.* To give an implementation of the  $H_{mod_r}$  hash function, we use  $k_2$ -bit truncation of the *SHA256* hash from example 47, and define a hash into  $\mathbb{Z}_{23}$  as follows:

$$H_{mod_{23}, k_2} : \{0, 1\}^* \rightarrow \mathbb{Z}_{23} : \\ s \mapsto \left( SHA256(s)_0 \cdot 2^0 + SHA256(s)_1 \cdot 2^1 + \dots + SHA256(s)_{k_2} \cdot 2^{k_2} \right) \bmod 23$$

We want to use various instantiations of  $k_2$  to visualize the impact of truncation length on the distribution of the hashes in  $\mathbb{Z}_{23}$ . We can invoke Sage to implement it as follows:

```
sage: import hashlib
sage: Z23 = Integers(23)
sage: def Hash_mod23(x, k2):
.....:     hasher = hashlib.sha256(x.encode('utf-8'))
.....:     digest = hasher.hexdigest()
.....:     d = ZZ(digest, base=16)
.....:     d = d.str(2)[-k2:]
.....:     d = ZZ(d, base=2)
.....:     return Z23(d)
```

We can then use Sage to apply this function to a large set of input values in order to plot visualizations of the distribution over the set  $\{0, \dots, 22\}$  for various values of  $k_2$ , by counting the number of times it maps onto each number in a loop of 100000 hashes. We get the following plot:



2171

2172 A third method that can sometimes be found in implementations is the so-called “**try-and-**  
 2173 **increment**” method. To understand this method, we define an integer  $z \in \mathbb{Z}$  from any hash  
 2174 value  $H(s)$  as we did in the previous methods, that is, we define  $z = H(s)_0 \cdot 2^0 + H(s)_1 \cdot 2^1 +$   
 2175  $\dots + H(s)_{k-1} \cdot 2^k$ .

2176 Hashing into  $\mathbb{Z}_r$  is then achievable by first computing  $z$ , and then trying to see if  $z \in \mathbb{Z}_r$ . If  
 2177 it is, then the hash is done; if not, the string  $s$  is modified in a deterministic way and the process  
 2178 is repeated until a suitable number  $z$  is found. A suitable, deterministic modification could be  
 2179 to concatenate the original string by some bit counter. A “try-and-increment” algorithm would  
 then work like in algorithm 5.

check  
reference

---

**Algorithm 5** Hash-to- $\mathbb{Z}_n$ 


---

**Require:**  $r \in \mathbb{Z}$  with  $r.\text{nbits}() = k$  and  $s \in \{0, 1\}^*$

**procedure** TRY-AND-INCREMENT( $r, k, s$ )

$c \leftarrow 0$

**repeat**

$s' \leftarrow s || c\_bits()$

$z \leftarrow H(s')_0 \cdot 2^0 + H(s')_1 \cdot 2^1 + \dots + H(s')_k \cdot 2^k$

$c \leftarrow c + 1$

**until**  $z < r$

**return**  $x$

**end procedure**

**Ensure:**  $z \in \mathbb{Z}_r$

---

2180

2181 Depending on the parameters, this method can be very efficient. In fact, if  $k$  is sufficiently  
 2182 large and  $r$  is close to  $2^{k+1}$ , the probability for  $z < r$  is very high and the repeat loop will almost  
 2183 always be executed a single time only. A drawback is, however, that the probability of having  
 2184 to execute the loop multiple times is not zero.

2185 Once some hash function into modular arithmetics is found, it can often be combined with  
 2186 additional techniques to hash into more general finite cyclic groups. The following paragraphs  
 2187 describe a few of those methods widely adopted in SNARK development.

2188 **Pedersen Hashes** The so-called **Pedersen hash function** [?] provides a way to map binary  
 2189 inputs of fixed size  $k$  onto elements of finite cyclic groups that avoids discrete log relations

between the images as they occur in the naive approach XXX. Combining it with a classical hash function provides a hash function that maps strings of arbitrary length onto group elements.

To be more precise, let  $j$  be an integer,  $\mathbb{G}$  a finite cyclic group of order  $r$  and  $\{g_1, \dots, g_j\} \subset \mathbb{G}$  a uniform randomly generated set of generators of  $\mathbb{G}$ . Then **Pedersen's hash function** is defined as follows:

$$H_{Ped} : (\mathbb{Z}_r)^j \rightarrow \mathbb{G} : (x_1, \dots, x_j) \mapsto \prod_{i=1}^j g_i^{x_i} \quad (4.24)$$

It can be shown that Pedersen's hash function is collision-resistant under the assumption that  $\mathbb{G}$  is a DL-A group. However, it is important to note that Pedersen hashes cannot be assumed to be **pseudorandom** and should therefore not be used where a hash function serves as an approximation of a random **oracle**. will these be explained in the initial chapters?

From an implementation perspective, it is important to derive the set of generators  $\{g_1, \dots, g_j\}$  in such a way that they are as uniform and random as possible. In particular, any known discrete log relation between two generators, that is, any known  $x \in \mathbb{Z}_r$  with  $g_h = (g_i)^x$  must be avoided.

To see how Pedersen hashes can be used to define an actual hash-to-group function according to our definition, we can use any of the hash-to- $\mathbb{Z}_r$  functions as we have derived them in equation 4.22.

## MimC Hashes [?]

**Pseudorandom Functions in DDH-A groups** As noted in above, Pederson's hash function does not have the properties a random function and should therefore not be instantiated as such. To see an example of a random oracle function in groups where the decisional Diffie–Hellman construction is assumed to hold true, let  $\mathbb{G}$  be a DDH-A group of order  $r$  with generator  $g$  and  $\{a_0, a_1, \dots, a_k\} \subset \mathbb{Z}_r^*$  a uniform randomly generated set of numbers invertible in modular  $r$  arithmetics. Then a pseudo-random function is given by the as follows:

$$F_{rand} : \{0, 1\}^{k+1} \rightarrow \mathbb{G} : (b_0, \dots, b_k) \mapsto g^{b_0 \cdot \prod_{i=1}^k a_i^{b_i}} \quad (4.25)$$

Of course, if  $H : \{0, 1\}^* \rightarrow \{0, 1\}^{k+1}$  is a random oracle, then the concatenation of  $F_{rand}$  and  $H$  also defines a random oracle

$$H_{rand, \mathbb{G}} : \{0, 1\}^* \rightarrow \mathbb{G} : s \mapsto F_{rand}(H(s)) \quad (4.26)$$

## 4.2 Commutative Rings

In the previous section we have seen that integers are a commutative group with respect to integer addition, but as we know there are in fact two arithmetic operations defined on integers: addition and multiplication. However, in contrast to addition, multiplication does not define a group structure, given that integers generally don't have multiplicative inverses. Configurations like these constitute so-called **commutative rings with unit** and the following definition will make the structure explicit:

**Definition 4.2.0.1** (Commutative ring with unit). A **commutative ring with unit**  $(R, +, \cdot, 1)$  is a set  $R$  provided with two maps  $+: R \times R \rightarrow R$  and  $\cdot: R \times R \rightarrow R$ , called **addition** and **multiplication** and an element  $1 \in R$ , called the **unit**, such that the following conditions hold:

- $(R, +)$  is a commutative group, where the neutral element is denoted with 0.
- **Commutativity of multiplication:**  $r_1 \cdot r_2 = r_2 \cdot r_1$  for all  $r_1, r_2 \in R$ .

- **Multiplicative neutral unit** :  $1 \cdot g = g$  for all  $g \in R$ .
- **Associativity**: For every  $g_1, g_2, g_3 \in \mathbb{G}$  the equation  $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$  holds.
- **Distributivity**: For all  $g_1, g_2, g_3 \in R$  the distributive law  $g_1 \cdot (g_2 + g_3) = g_1 \cdot g_2 + g_1 \cdot g_3$  holds.

*Notation and Symbols* 6. Since we are exclusively concerned with commutative rings in this book, we often just call them rings, keeping the notation of commutativity implicit. A set  $R$  with two maps  $+$  and  $\cdot$  that satisfies all previously mentioned rules, except for the commutativity law of the multiplication is called a non-commutative ring.

If there is no risk of ambiguity (about what the addition and multiplication maps of a ring are), we frequently drop the symbols  $+$  and  $\cdot$  and simply write  $R$  as notation for the ring, keeping those maps implicit. In this case we also say that  $R$  is of ring type, indicating that  $R$  is not simply a set but a set together with an addition and a multiplication map.

*Example 51* (The ring of integers). The set  $\mathbb{Z}$  of integers with the usual addition and multiplication is the archetypical example of a commutative ring with unit 1.

**sage: ZZ**

**Integer Ring**

194

195

*Example 52* (Underlying commutative group of a ring). Every commutative ring with unit  $(R, +, \cdot, 1)$  gives rise to a group, if we disregard multiplication.

The following example is somewhat unusual, but we encourage you to think through it because it helps to detach the mind from familiar styles of computation and concentrate on the abstract algebraic explanation.

*Example 53*. Let  $S := \{\bullet, \star, \odot, \otimes\}$  be a set that contains four elements, and let addition and multiplication on  $S$  be defined as follows:

$\cup$	$\bullet$	$\star$	$\odot$	$\otimes$		$\circ$	$\bullet$	$\star$	$\odot$	$\otimes$
$\bullet$	$\bullet$	$\star$	$\odot$	$\otimes$		$\bullet$	$\bullet$	$\bullet$	$\bullet$	$\bullet$
$\star$	$\star$	$\odot$	$\otimes$	$\bullet$		$\star$	$\bullet$	$\star$	$\odot$	$\otimes$
$\odot$	$\odot$	$\otimes$	$\bullet$	$\star$		$\odot$	$\bullet$	$\odot$	$\bullet$	$\odot$
$\otimes$	$\otimes$	$\bullet$	$\star$	$\odot$		$\otimes$	$\bullet$	$\otimes$	$\odot$	$\star$

Then  $(S, \cup, \circ, \star)$  is a ring with unit  $\star$  and zero  $\bullet$ . It therefore makes sense to ask for solutions to equations like this one: Find  $x \in S$  such that

$$\otimes \circ (x \cup \odot) = \star$$

To see how such a “moonmath equation” can be solved, we have to keep in mind that rings behaves mostly like normal numbers when it comes to bracketing and computation rules. The only differences are the symbols, and the actual way to add and multiply them. With this in



mind, we solve the equation for  $x$  in the “usual way”<sup>1</sup>:

$$\begin{array}{ll}
 \otimes \circ (x \cup \odot) = \star & \# \text{ apply the distributive law} \\
 \otimes \circ x \cup \otimes \circ \odot = \star & \# \otimes \circ \odot = \odot \\
 \otimes \circ x \cup \odot = \star & \# \text{ concatenate the } \cup \text{ inverse of } \odot \text{ to both sides} \\
 \otimes \circ x \cup \odot \cup -\odot = \star \cup -\odot & \# \odot \cup -\odot = \bullet \\
 \otimes \circ x \cup \bullet = \star \cup -\odot & \# \bullet \text{ is the } \cup \text{ neutral element} \\
 \otimes \circ x = \star \cup -\odot & \# \text{ for } \cup \text{ we have } -\odot = \odot \\
 \otimes \circ x = \star \cup \odot & \# \star \cup \odot = \otimes \\
 \otimes \circ x = \otimes & \# \text{ concatenate the } \circ \text{ inverse of } \otimes \text{ to both sides} \\
 (\otimes)^{-1} \circ \otimes \circ x = (\otimes)^{-1} \circ \otimes & \# \text{ multiply with the multiplicative inverse} \\
 \star \circ x = \star & \\
 x = \star & 
 \end{array}$$

2250 So, even though this equation looked really alien at first glance, we could solve it basically  
 2251 exactly the way we solve “normal” equations containing numbers.

2252 Note, however, that whenever a multiplicative inverse would be needed to solve an equation  
 2253 in the usual way in a ring, things can be very different than most of us are used to. For example,  
 2254 the following equation cannot be solved for  $x$  in the usual way, since there is no multiplicative  
 2255 inverse for  $\odot$  in our ring.

$$\odot \circ x = \otimes \quad (4.27)$$

2256 We can confirm this by looking at the multiplication table to see that no such  $x$  exists.

2257 As another example, the following equation does not have a single solution but two:  $x \in$   
 2258  $\{\star, \otimes\}$ .

$$\odot \circ x = \odot \quad (4.28)$$

2259 Having no solution or two solutions is certainly not something to expect from types like the  
 2260 rational numbers  $\mathbb{Q}$ .

2261 *Example 54* (Ring of Polynomials). Considering the definition of polynomials from 3.4 again,  
 2262 we notice that what we have informally called the type  $R$  of the coefficients must in fact be a  
 2263 commutative ring with a unit, since we need addition, multiplication, commutativity and the  
 2264 existence of a unit for  $R[x]$  to have the properties we expect.

2265 In fact if we consider  $R$  to be a ring and we define addition and multiplication of polyno-  
 2266 mials as in 3.23, the set  $R[x]$  is a commutative ring with a unit, where the polynomial 1 is the  
 2267 multiplicative unit. We call this ring the **ring of polynomials with coefficients in  $R$** .

2268 **sage: ZZ['x']** 196  
 2269 **Univariate Polynomial Ring in x over Integer Ring** 197

2270 *Example 55* (Ring of modular  $n$  arithmetic). Let  $n$  be a modulus and  $(\mathbb{Z}_n, +, \cdot)$  the set of all re-  
 2271 mainder classes of integers modulo  $n$ , with the projection of integer addition and multiplication  
 2272 as defined in 3.3. Then  $(\mathbb{Z}_n, +, \cdot)$  is a commutative ring with unit 1.

<sup>1</sup>Note that there are more efficient ways to solve this equation. The point of our computation is to show how the axioms of a ring can be used to solve the equation



2273 **sage: Integers(6)**

198

2274 **Ring of integers modulo 6**

199

2275 *Example 56* (Polynomial evaluation in the exponent of group generators). As we show in 6.2.3,  
 2276 a key insights in many zero knowledge protocols is the ability to encode computations as poly-  
 2277 nomials and then to hide the information of that computation by evaluating the polynomial "in  
 2278 the exponent" of certain cryptographic groups 8.2.

To understand the underlying principle of this idea, consider the exponential map 44 again. If  $\mathbb{G}$  is a finite cyclic group of order  $n$  with generator  $g \in \mathbb{G}$ , then the ring structure of  $(\mathbb{Z}_n, +, \cdot)$  corresponds to the group structure of  $\mathbb{G}$  in the following way:

$$g^{x+y} = g^x \cdot g^y \quad g^{x \cdot y} = (g^x)^y \quad \text{for all } x, y \in \mathbb{Z}_n \quad (4.29)$$

This correspondence allows polynomials with coefficients in  $\mathbb{Z}_n$  to be evaluated "in the exponent" of a group generator. To see what this means, let  $p \in \mathbb{Z}_n[x]$  be a polynomial with  $p(x) = a_m \cdot x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0$  and let  $s \in \mathbb{Z}_n$  be an evaluation point. Then the previously defined exponential laws 4.29 imply the following identity:

$$\begin{aligned} g^{p(s)} &= g^{a_m \cdot s^m + a_{m-1}s^{m-1} + \dots + a_1s + a_0} \\ &= \left(g^{s^m}\right)^{a_m} \cdot \left(g^{s^{m-1}}\right)^{a_{m-1}} \cdot \dots \cdot (g^s)^{a_1} \cdot g^{a_0} \end{aligned} \quad (4.30)$$

2279 Utilizing these identities, it is possible to evaluate any polynomial  $p$  of degree  $\deg(p) \leq m$  at a  
 2280 "secret" evaluation point  $s$  in the exponent of  $g$  without any knowledge about  $s$ , assuming that  
 2281  $\mathbb{G}$  is a DL-group. To see this assume that the set  $\{g, g^s, g^{s^2}, \dots, g^{s^m}\}$  is given, but  $s$  is unknown.  
 2282 Then  $g^{p(s)}$  can be computed using 4.30, however it is not feasible to compute  $s$ .

*Example 57.* To give an example of the evaluation of a polynomial in the exponent of a finite cyclic group, consider the exponential map from example 36:

$$3^{(\cdot)} : \mathbb{Z}_4 \rightarrow \mathbb{Z}_5^* x \mapsto 3^x$$

Choosing the polynomial  $p(x) = 2x^2 + 3x + 1$  from  $\mathbb{Z}_4[x]$ , we first evaluate the polynomial at the point  $s = 2$  and then write the result into the exponent 3 as follows:

$$\begin{aligned} 3^{p(2)} &= 3^{2 \cdot 2^2 + 3 \cdot 2 + 1} \\ &= 3^{2 \cdot 0 + 2 + 1} \\ &= 3^3 \\ &= 2 \end{aligned}$$

This was possible, because we had access to the evaluation point 2. On the other hand, if we only had access to the set  $\{3, 4, 1\}$  and we knew that this set represents the set  $\{3, 3^s, 3^{s^2}\}$  for some secret value  $s$ , we could evaluate  $p$  at the point  $s$  in the exponent of 3 as

$$\begin{aligned} 3^{p(s)} &= 1^2 \cdot 4^3 \cdot 3^1 \\ &= 1 \cdot 4 \cdot 3 \\ &= 2 \end{aligned}$$

2283 Both computations agree, since the secret point  $s$  was equal to 2 in this example. However the  
 2284 second evaluation was possible without any knowledge about  $s$ .

**Hashing to Commutative Rings** As we have seen in XXX, various constructions for hashing-to-groups are known and used in applications. As commutative rings are **Abelian groups**, when we disregard the multiplicative structure, hash-to-group constructions can be applied for hashing into commutative rings, too. This is possible in general, as the **codomain of a general hash function**  $\{0, 1\}^*$  is just the set of binary strings of arbitrary but finite length, which has no algebraic structure that the hash function must respect.

add reference

codomain groups

## 4.3 Fields

We started this chapter with the definition of a group (section 4.1), which we then expanded into the definition of a commutative ring with a unit (section 4.2). Such rings generalize the behavior of integers. In this section, we will look at those special cases of commutative rings where every element other than the neutral element of addition has a multiplicative inverse. Those structures behave very much like the rational numbers  $\mathbb{Q}$ . Rational numbers are, in a sense, an extension of the ring of integers, that is, they are constructed by including newly defined multiplicative inverses (fractions) to the integers.

**Definition 4.3.0.1 (Field).** A **field**  $(\mathbb{F}, +, \cdot, 1)$  is a set  $\mathbb{F}$  provided with two maps  $+: \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$  and  $\cdot: \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$ , called **addition** and **multiplication**, such that the following conditions hold:

- $(\mathbb{F}, +)$  is a commutative group, where the neutral element is denoted by 0.
- $(\mathbb{F} \setminus \{0\}, \cdot)$  is a commutative group, where the neutral element is denoted by 1.
- (Distributivity) For all  $g_1, g_2, g_3 \in \mathbb{F}$  the distributive law  $g_1 \cdot (g_2 + g_3) = g_1 \cdot g_2 + g_1 \cdot g_3$  holds.

**Notation and Symbols 7.** If there is no risk of ambiguity (about what the addition and multiplication maps of a ring are), we frequently drop the symbols  $+$  and  $\cdot$  and simply write  $\mathbb{F}$  as notation for the field, keeping those maps implicit. In this case we also say that  $\mathbb{F}$  is of field type, indicating that  $\mathbb{F}$  is not simply a set but a set together with an addition and a multiplication map.

Moreover, we use the symbol  $\mathbb{F}^*$  to describe the multiplicative group of the field, that is, the set of elements with multiplication as the group law, excluding the neutral element of addition.

The **characteristic** of a field  $\mathbb{F}$ , represented as  $\text{char}(\mathbb{F})$ , is the smallest natural number  $n \geq 1$  for which the  $n$ -fold sum of 1 equals zero, i.e. for which  $\sum_{i=1}^n 1 = 0$ . If such an  $n > 0$  exists, the field is also said to have a **finite characteristic**. If, on the other hand, every finite sum of 1 is such that it is not equal to zero, then the field is defined to have characteristic 0. **S: Tried to disambiguate the scope of negation between 1.** “It is true of every finite sum of 1 that it is not equal to 0” and 2. “It is not true of every finite sum of 1 that it is equal to 0” From the example below, it looks like 1. is the intended meaning here, correct?

Check change of wording

**Example 58 (Field of rational numbers).** Probably the best known example of a field is the set of rational numbers  $\mathbb{Q}$  together with the usual definition of addition, subtraction, multiplication and division. Since there is no natural number  $n \in \mathbb{N}$ , such that  $\sum_{j=0}^n 1 = 0$  in the set of rational numbers, the characteristic of the field  $\mathbb{Q}$  is given by  $\text{char}(\mathbb{Q}) = 0$ .

**sage: QQ** 200  
**Rational Field** 201  
**sage: QQ(1/5) # Get an element from the field of rational numbers** 202

2327 **1/5** 203  
 2328 **sage: QQ(1/5) / QQ(3) # Division** 204  
 2329 **1/15** 205

2330 *Example 59* (Field with two elements). It can be shown that, in any field, the neutral element  
 2331 of addition 0 must be different from the neutral element of multiplication 1, that is,  $0 \neq 1$   
 2332 always holds in a field. From this, it follows that the smallest field must contain at least two  
 2333 elements. As the following addition and multiplication tables show, there is indeed a field with  
 2334 two elements, which is usually called  $\mathbb{F}_2$ :

2335 Let  $\mathbb{F}_2 := \{0, 1\}$  be a set that contains two elements and let addition and multiplication on  
 2336  $\mathbb{F}_2$  be defined as follows:

2337

+	0	1		·	0	1
0	0	1		0	0	0
1	1	0		1	0	1

2338 Since  $1 + 1 = 0$  in the field  $\mathbb{F}_2$ , we know that the characteristic of  $\mathbb{F}_2$  given by  $\text{char}(\mathbb{F}_2) = 2$ .

2339 **sage: F2 = GF(2)** 206  
 2340 **sage: F2(1) # Get an element from GF(2)** 207  
 2341 **1** 208  
 2342 **sage: F2(1) + F2(1) # Addition** 209  
 2343 **0** 210  
 2344 **sage: F2(1) / F2(1) # Division** 211  
 2345 **1** 212

2346 *Example 60.* Both the real numbers  $\mathbb{R}$  as well as the complex numbers  $\mathbb{C}$  are well known ex-  
 2347 amples of fields.

2348 *Exercise 41.* Consider the ring of modular 5 arithmetics  $(\mathbb{Z}_5, +, \cdot)$  from example 14. Show that  
 2349  $(\mathbb{Z}_5, +, \cdot)$  is a field. What is the characteristic of  $\mathbb{Z}_5$ ? Proof that the equation  $a \cdot x = b$  has only a  
 2350 single solution  $x \in \mathbb{Z}_5$  for any given  $a, b \in \mathbb{Z}_5^*$ .

2351 *Exercise 42.* Consider the ring of modular 6 arithmetics  $(\mathbb{Z}_6, +, \cdot)$  from example 9. Show that  
 2352  $(\mathbb{Z}_6, +, \cdot)$  is not a field.

### 2353 4.3.1 Prime fields

2354 As we have seen in the various examples of the previous sections, modular arithmetics behaves  
 2355 similarly to the ordinary arithmetics of integers in many ways. This is due to the fact that  
 2356 remainder class sets  $\mathbb{Z}_n$  are commutative rings with units 55.

2357 However, we have also seen in 35 that, whenever the modulus is a prime number, every  
 2358 remainder class other than the zero class has a modular multiplicative inverse. This is an impor-  
 2359 tant observation, since it immediately implies that, in case the modulus is a prime number, the  
 2360 remainder class set  $\mathbb{Z}_n$  is not just a ring but actually a **field**. Moreover, since  $\sum_{j=0}^n 1 = 0$  in  $\mathbb{Z}_n$ ,  
 2361 we know that those fields have the finite characteristic  $n$ .

2362 To distinguish this important case from arbitrary remainder class rings, we write  $(\mathbb{F}_p, +, \cdot)$   
 2363 for the field of all remainder classes for a prime number modulus  $p \in \mathbb{P}$  and call it the **prime**  
 2364 **field** of characteristic  $p$ .

2365 Prime fields are the foundation for many of the contemporary algebra-based cryptographic  
 2366 systems, as they have many desirable properties. One of them is that any prime field of char-  
 2367 acteristic  $p$  contain exactly  $p$  elements which can be represented on a computer with not more

Expand  
on this?

check  
reference

then  $\log_2(p)$  many bits. On the other hand fields like the rational numbers, require a potentially unbounded amount of bits for any full-precision representation.

Since prime fields are special cases of modular arithmetic rings, addition and multiplication can be computed by first doing normal integer addition and multiplication, and then considering the remainder in Euclidean division by  $p$  as the result. For any prime field element  $x \in \mathbb{F}_p$ , its additive inverse (the negative) is given by  $-x = p - x \bmod p$ . For  $x \neq 0$  the multiplicative inverse always exists and is given by  $x^{-1} = x^{p-2}$ . Division is then defined by multiplication with the multiplicative inverse as explained in 3.3. Alternatively the multiplicative inverse can be computed using the Extended Euclidean Algorithm as explained in 3.19.

*Example 61.* The smallest field is the field  $\mathbb{F}_2$  of characteristic 2 as we have seen in example 59. It is the prime field of the prime number 2.

*Example 62.* To summarize the basic aspects of computation in prime fields, let us consider the prime field  $\mathbb{F}_5$  and simplify the following expression:

$$\left(\frac{2}{3} - 2\right) \cdot 2$$

A first thing to note is that since  $\mathbb{F}_5$  is a field, all rules are identical to the rules we learned in school when we were dealing with rational, real or complex numbers. This means we can use e.g. bracketing (distributivity) or addition as usual:

$$\begin{aligned} \left(\frac{2}{3} - 2\right) \cdot 2 &= \frac{2}{3} \cdot 2 - 2 \cdot 2 && \# \text{ distributive law} \\ &= \frac{2 \cdot 2}{3} - 2 \cdot 2 && 4 \bmod 5 = 4 \\ &= \frac{4}{3} - 4 && \# \text{ multiplicative inverse of 3 is } 3^{5-2} \bmod 5 = 2 \\ &= 4 \cdot 2 - 4 && \# \text{ additive inverse of 4 is } 5 - 4 = 1 \\ &= 4 \cdot 2 + 1 && 8 \bmod 5 = 3 \\ &= 3 + 1 && 4 \bmod 5 = 4 \\ &= 4 \end{aligned}$$

In this computation, we computed the multiplicative inverse of 3 using the identity  $x^{-1} = x^{p-2}$  in a prime field. This is impractical for large prime numbers. Recall that another way of computing the multiplicative inverse is the Extended Euclidean Algorithm (see 3.10). To refresh our memory, the algorithm solves the equation  $x^{-1} \cdot 3 + t \cdot 5 = 1$ , for  $x^{-1}$ , even though in this case  $t$  is irrelevant. We get:

k	$r_k$	$x_k^{-1}$	$t_k = (r_k - s_k \cdot 3) \bmod 5$
0	3	1	.
1	5	0	.
2	3	1	.
3	2	-1	.
4	1	2	.

So the multiplicative inverse of 3 in  $\mathbb{Z}_5$  is 2, and, indeed, if compute  $3 \cdot 2$ , we get 1 in  $\mathbb{F}_5$ .

**Square Roots** In this part, we deal with square numbers, also called **quadratic residues** and **square roots** in prime fields. This is of particular importance in our studies on elliptic curves, as only square numbers can actually be points on an elliptic curve.

To make the intuition of quadratic residues and roots precise, let  $p \in \mathbb{P}$  be a prime number and  $\mathbb{F}_p$  its associated prime field. Then a number  $x \in \mathbb{F}_p$  is called a **square root** of another number  $y \in \mathbb{F}_p$ , if  $x$  is a solution to the following equation:

$$x^2 = y \quad (4.31)$$

In this case,  $y$  is called a **quadratic residue**. On the other hand, if  $y$  is given and the quadratic equation has no solution  $x$ , we call  $y$  a **quadratic non-residue**. For any  $y \in \mathbb{F}_p$ , we denote the set of all square roots of  $y$  in the prime field  $\mathbb{F}_p$  as follows:

$$\sqrt{y} := \{x \in \mathbb{F}_p \mid x^2 = y\} \quad (4.32)$$

If  $y$  is a quadratic non-residue, then  $\sqrt{y} = \emptyset$  (an empty set), and if  $y = 0$ , then  $\sqrt{y} = \{0\}$ .

Informally speaking, quadratic residues are numbers such that we can take the square root of them, while quadratic non-residues are numbers that don't have square roots. The situation therefore parallels the familiar case of integers, where some integers like 4 or 9 have square roots and others like 2 or 3 don't (as integers).

It can be shown that, in any prime field, every non zero element has either no square root or two of them. We adopt the convention to call the smaller one (when interpreted as an integer) as the **positive** square root and the larger one as the **negative**. This makes sense, as the larger one can always be computed as the modulus minus the smaller one, which is the definition of the negative in prime fields.

*Example 63* (Quadratic (Non)-Residues and roots in  $\mathbb{F}_5$ ). Let us consider our example prime field  $\mathbb{F}_5$  again. All square numbers can be found on the main diagonal of the multiplication table in example 14 on page 28. As you can see, in  $\mathbb{F}_5$  only the numbers 0, 1 and 4 have square roots and we get  $\sqrt{0} = \{0\}$ ,  $\sqrt{1} = \{1, 4\}$ ,  $\sqrt{2} = \emptyset$ ,  $\sqrt{3} = \emptyset$  and  $\sqrt{4} = \{2, 3\}$ . The numbers 0, 1 and 4 are therefore quadratic residues, while the numbers 2 and 3 are quadratic non-residues.

In order to describe whether an element of a prime field is a square number or not, the so-called **Legendre symbol** can sometimes be found in the literature, which is why we will summarize it here:

Let  $p \in \mathbb{P}$  be a prime number and  $y \in \mathbb{F}_p$  an element from the associated prime field. Then the *Legendre symbol* of  $y$  is defined as follows:

$$\left(\frac{y}{p}\right) := \begin{cases} 1 & \text{if } y \text{ has square roots} \\ -1 & \text{if } y \text{ has no square roots} \\ 0 & \text{if } y = 0 \end{cases} \quad (4.33)$$

*Example 64.* Looking at the quadratic residues and non residues in  $\mathbb{F}_5$  from example 14 again, we can deduce the following Legendre symbols, from example XXX.

$$\left(\frac{0}{5}\right) = 0, \quad \left(\frac{1}{5}\right) = 1, \quad \left(\frac{2}{5}\right) = -1, \quad \left(\frac{3}{5}\right) = -1, \quad \left(\frac{4}{5}\right) = 1.$$

The Legendre symbol provides a criterion to decide whether or not an element from a prime field has a quadratic root or not. This, however, is not just of theoretical use: The so-called **Euler criterion** provides a compact way to actually compute the Legendre symbol. To see that, let  $p \in \mathbb{P}_{\geq 3}$  be an odd prime number and  $y \in \mathbb{F}_p$ . Then the Legendre symbol can be computed as follows:

$$\left(\frac{y}{p}\right) = y^{\frac{p-1}{2}}. \quad (4.34)$$

S: are we introducing elliptic curves in section 1 or 2?

check reference

check reference

add reference

*Example 65.* Looking at the quadratic residues and non residues in  $\mathbb{F}_5$  from example 14 again, we can compute the following Legendre symbols using the Euler criterion:

check  
reference

$$\begin{aligned}\left(\frac{0}{5}\right) &= 0^{\frac{5-1}{2}} = 0^2 = 0 \\ \left(\frac{1}{5}\right) &= 1^{\frac{5-1}{2}} = 1^2 = 1 \\ \left(\frac{2}{5}\right) &= 2^{\frac{5-1}{2}} = 2^2 = 4 = -1 \\ \left(\frac{3}{5}\right) &= 3^{\frac{5-1}{2}} = 3^2 = 4 = -1 \\ \left(\frac{4}{5}\right) &= 4^{\frac{5-1}{2}} = 4^2 = 1\end{aligned}$$

*Exercise 43.* Consider the prime field  $\mathbb{F}_{13}$ . Find the set of all pairs  $(x, y) \in \mathbb{F}_{13} \times \mathbb{F}_{13}$  that satisfy the equation

$$x^2 + y^2 = 1 + 7 \cdot x^2 \cdot y^2$$

2422 **Exponentiation** TO APPEAR...

write  
paragraph  
on expo-  
nentiation

2423 **Hashing into prime fields**

2424 An important problem in SNARK development is the ability to hash to (various subsets) of  
2425 elliptic curves. As we will see in XXX, those curves are often defined over prime fields, and  
2426 hashing to a curve might start with hashing to the prime field. It is therefore important to  
2427 understand how to hash into prime fields.

add refer-  
ence

2428 On pages 54–57, we looked at a few methods of hashing into the residue class rings  $\mathbb{Z}_n$  for  
2429 arbitrary  $n > 1$ . As prime fields are just special instances of those rings, all methods for hashing  
2430 into  $\mathbb{Z}_n$  functions can be used for hashing into prime fields, too.

check  
reference

2431 **MiMC Hash functions** As we will see in XXX,

2432 To define a MiMC hash function, let  $\mathbb{F}_p$  be a prime field with prime modulus  $p \in \mathbb{P}$ , let  $n$  be  
2433 the smallest natural number, such that  $\gcd(n, p-1) = 1$ . Let  $r$  be the smallest integer greater  
2434 than or equal to  $\frac{\log(p)}{\log_2(3)}$  and let  $C = \{c_i \in \mathbb{F}_p \mid 0 \leq i \leq r\}$  be a set of randomly generated field  
2435 elements. The definition of the MiMC hash function then starts with an invertible map

$$E(\cdot) : \mathbb{F}_p \rightarrow \mathbb{F}_p \quad x \mapsto F_{r-1}(\cdots F_1(F_0(x)) \cdots) \quad (4.35)$$

2436 where  $F_i(x) = (x + c_i)^n$

## 2437 4.3.2 Extension Fields

2438 Prime fields, defined in the previous section, are the basic building blocks for cryptography in  
2439 general and SNARKs in particular.

2440 However, as we will see in XXX so-called **pairing-based** SNARK systems are crucially  
2441 dependent on **group pairings** XXX defined over the group of rational points of elliptic curves.  
2442 For those pairings to be non-trivial, the elliptic curve must not only be defined over a prime  
2443 field, but over a so-called **extension field** of a given prime field.

add refer-  
ence

group  
pairings

We therefore have to understand field extensions. First note that the field  $\mathbb{F}'$  is called an **extension** of a field  $\mathbb{F}$  if  $\mathbb{F}$  is a subfield of  $\mathbb{F}'$ , that is,  $\mathbb{F}$  is a subset of  $\mathbb{F}'$  and restricting the addition and multiplication laws of  $\mathbb{F}'$  to the subset  $\mathbb{F}$  recovers the appropriate laws of  $\mathbb{F}$ .

Now it can be shown that whenever  $p \in \mathbb{P}$  is a prime and  $m \in \mathbb{N}$  a natural number, then there is a field  $\mathbb{F}_{p^m}$  with characteristic  $p$  and  $p^m$  elements such that  $\mathbb{F}_{p^m}$  is an extension field of the prime field  $\mathbb{F}_p$ .

Similarly to the way prime fields  $\mathbb{F}_p$  are generated by starting with the ring of integers and then dividing by a prime number  $p$  and keeping the remainder, prime field extensions  $\mathbb{F}_{p^m}$  are generated by starting with the ring  $\mathbb{F}_p[x]$  of polynomials and then dividing them by an irreducible polynomial of degree  $m$  and keeping the remainder.

To be more precise, let  $P \in \mathbb{F}_p[x]$  be an irreducible polynomial of degree  $m$  with coefficients from the given prime field  $\mathbb{F}_p$ . Then the underlying set  $\mathbb{F}_{p^m}$  of the extension field is given by the set of all polynomials with a degree less than  $m$ :

$$\mathbb{F}_{p^m} := \{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \dots + a_1x + a_0 \mid a_i \in \mathbb{F}_p\} \quad (4.36)$$

This can be shown to be the set of all remainders when dividing any polynomial  $Q \in \mathbb{F}_p[x]$  by  $P$ , consequently, elements of the extension field are polynomials of degree less than  $m$ . This is analogous to how  $\mathbb{F}_p$  is the set of all remainders when dividing integers by  $p$ .

Addition is inherited from  $\mathbb{F}_p[x]$ , which means that addition on  $\mathbb{F}_{p^m}$  is defined like normal addition of polynomials:

$$+ : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \rightarrow \mathbb{F}_{p^m}, \left( \sum_{j=0}^m a_j x^j, \sum_{j=0}^m b_j x^j \right) \mapsto \sum_{j=0}^m (a_j + b_j) x^j \quad (4.37)$$

We can see that the neutral element is (the polynomial) 0, and that the additive inverse is given by the polynomial with all negative coefficients.

Multiplication is inherited from  $\mathbb{F}_p[x]$ , too, but we have to divide the result by our modulus polynomial  $P$  whenever the degree of the resulting polynomial is equal or greater to  $m$ :

$$\cdot : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \rightarrow \mathbb{F}_{p^m}, \left( \sum_{j=0}^m a_j x^j, \sum_{j=0}^m b_j x^j \right) \mapsto \left( \sum_{n=0}^{2m} \sum_{i=0}^n a_i b_{n-i} x^n \right) \bmod P \quad (4.38)$$

We can see that the neutral element is (the polynomial) 1. It is, however, not obvious from this definition how the multiplicative inverse looks.

We can easily see from the definition of  $\mathbb{F}_{p^m}$  that the field is of characteristic  $p$ , since the multiplicative neutral element 1 is equivalent to the multiplicative element 1 from the underlying prime field, and hence  $\sum_{j=0}^p 1 = 0$ . Moreover,  $\mathbb{F}_{p^m}$  is finite and contains  $p^m$  many elements, since elements are polynomials of degree  $< m$ , and every coefficient  $a_j$  can have a  $p$  number of different values. In addition, we see that the prime field  $\mathbb{F}_p$  is a subfield of  $\mathbb{F}_{p^m}$  that occurs when we restrict the elements of  $\mathbb{F}_{p^m}$  to polynomials of degree zero.

One key point is that the construction of  $\mathbb{F}_{p^m}$  depends on the choice of an irreducible polynomial, and, in fact, different choices will give different multiplication tables, since the remainders from dividing a product by  $P$  will be different.

It can, however, be shown that the fields for different choices of  $P$  are **isomorphic**, which means that there is a one-to-one correspondence between all of them. Consequently, from an abstract point of view, they are the same thing. From an implementations point of view, however, some choices are preferable to others because they allow for faster computations.

To summarize, we have seen that when a prime field  $\mathbb{F}_p$  is given, any field  $\mathbb{F}_{p^m}$  constructed in the above manner is a field extension of  $\mathbb{F}_p$ . To be more general, a field  $\mathbb{F}_{p^{m_2}}$  is a field extension



2483 of a field  $\mathbb{F}_{p^{m_1}}$ , if and only if  $m_1$  divides  $m_2$ . From this, we can deduce that, for any given fixed  
 2484 prime number, there are nested sequences of fields whenever the power  $m_j$  divides the power  
 2485  $m_{j+1}$ , such that  $\mathbb{F}_{p^{m_j}}$  is a subfield of  $\mathbb{F}_{p^{m_{j+1}}}$ :

$$\mathbb{F}_p \subset \mathbb{F}_{p^{m_1}} \subset \cdots \subset \mathbb{F}_{p^{m_k}} \quad (4.39)$$

2486 To get a more intuitive picture of this, we construct an extension field of the prime field  $\mathbb{F}_3$   
 2487 in the following example, and we can see how  $\mathbb{F}_3$  sits inside that extension field.

*Example 66* (The Extension field  $\mathbb{F}_{3^2}$ ). In (XXX) we have constructed the prime field  $\mathbb{F}_3$ . In this example, we apply the definition of a field extension (page 66) to construct  $\mathbb{F}_{3^2}$ . We start by choosing an irreducible polynomial of degree 2 with coefficients in  $\mathbb{F}_3$ . We try  $P(t) = t^2 + 1$ . Possibly the fastest way to show that  $P$  is indeed irreducible is to just insert all elements from  $\mathbb{F}_3$  to see if the result is ever zero. We compute as follows:

$$P(0) = 0^2 + 1 = 1$$

$$P(1) = 1^2 + 1 = 2$$

$$P(2) = 2^2 + 1 = 1 + 1 = 2$$

This implies that  $P$  is irreducible. The set  $\mathbb{F}_{3^2}$  contains all polynomials of degrees lower than two, with coefficients in  $\mathbb{F}_3$ , which are precisely as listed below:

$$\mathbb{F}_{3^2} = \{0, 1, 2, t, t+1, t+2, 2t, 2t+1, 2t+2\}$$

2488 As expected, our extension field contains 9 elements. Addition is defined as addition of poly-  
 2489 nomials; for example  $(t+2) + (2t+2) = (1+2)t + (2+2) = 1$ . Doing this computation for all  
 2490 elements gives the following addition table

+	0	1	2	t	t+1	t+2	2t	2t+1	2t+2
0	0	1	2	t	t+1	t+2	2t	2t+1	2t+2
1	1	2	0	t+1	t+2	t	2t+1	2t+2	2t
2	2	0	1	t+2	t	t+1	2t+2	2t	2t+1
t	t	t+1	t+2	2t	2t+1	2t+2	0	1	2
t+1	t+1	t+2	t	2t+1	2t+2	2t	1	2	0
t+2	t+2	t	t+1	2t+2	2t	2t+1	2	0	1
2t	2t	2t+1	2t+2	0	1	2	t	t+1	t+2
2t+1	2t+1	2t+2	2t	1	2	0	t+1	t+2	t
2t+2	2t+2	2t	2t+1	2	0	1	t+2	t	t+1

2492 As we can see, the group  $(\mathbb{F}_3, +)$  is a subgroup of the group  $(\mathbb{F}_{3^2}, +)$ , obtained by only consid-  
 2493 ering the first three rows and columns of this table.

2494 As it was the case in previous examples, we can use the table to deduce the negative of any  
 2495 element from  $\mathbb{F}_{3^2}$ . For example, in  $\mathbb{F}_{3^2}$  we have  $-(2t+1) = t+2$ , since  $(2t+1) + (t+2) = 0$

Multiplication needs a bit more computation, as we first have to multiply the polynomials, and whenever the result has a degree  $\geq 2$ , we have to divide it by  $P$  and keep the remainder. To see how this works, let us compute the product of  $t+2$  and  $2t+2$  in  $\mathbb{F}_{3^2}$ :

$$\begin{aligned} (t+2) \cdot (2t+2) &= (2t^2 + 2t + t + 1) \bmod (t^2 + 1) \\ &= (2t^2 + 1) \bmod (t^2 + 1) & \# 2t^2 + 1 : t^2 + 1 &= 2 + \frac{2}{t^2 + 1} \\ &= 2 \end{aligned}$$

add refer-  
ence

check  
reference



2496 This means that the product of  $t + 2$  and  $2t + 2$  in  $\mathbb{F}_{3^2}$  is 2. Performing this computation for all  
 2497 elements gives the following multiplication table:

·	0	1	2	t	t+1	t+2	2t	2t+1	2t+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	t	t+1	t+2	2t	2t+1	2t+2
2	0	2	1	2t	2t+2	2t+1	t	t+2	t+1
t	0	t	2t	2	t+2	2t+2	1	t+1	2t+1
t+1	0	t+1	2t+2	t+2	2t	1	2t+1	2	t
t+2	0	t+2	2t+1	2t+2	1	t	t+1	2t	2
2t	0	2t	t	1	2t+1	t+1	2	2t+2	t+2
2t+1	0	2t+1	t+2	t+1	2	2t	2t+2	t	1
2t+2	0	2t+2	t+1	2t+1	t	2	t+2	1	2t

2499 As it was the case in previous examples, we can use the table to deduce the multiplicative  
 2500 inverse of any non-zero element from  $\mathbb{F}_{3^2}$ . For example, in  $\mathbb{F}_{3^2}$  we have  $(2t + 1)^{-1} = 2t + 2$ ,  
 2501 since  $(2t + 1) \cdot (2t + 2) = 1$ .

2502 From the multiplication table, we can also see that the only quadratic residues in  $\mathbb{F}_{3^2}$  are  
 2503 from the set  $\{0, 1, 2, t, 2t\}$ , with  $\sqrt{0} = \{0\}$ ,  $\sqrt{1} = \{1, 2\}$ ,  $\sqrt{2} = \{t, 2t\}$ ,  $\sqrt{t} = \{t + 2, 2t + 1\}$  and  
 2504  $\sqrt{2t} = \{t + 1, 2t + 2\}$ .

Since  $\mathbb{F}_{3^2}$  is a field, we can solve equations as we would for other fields, (such as rational numbers). To see that, let us find all  $x \in \mathbb{F}_{3^2}$  that solve the quadratic equation  $(t + 1)(x^2 + (2t + 2)) = 2$ . We compute as follows:

$$\begin{aligned}
 (t + 1)(x^2 + (2t + 2)) &= 2 && \# 2 \text{ distributive law} \\
 (t + 1)x^2 + (t + 1)(2t + 2) &= 2 \\
 (t + 1)x^2 + (t) &= 2 && \# 2 \text{ add the additive inverse of } t \\
 (t + 1)x^2 + (t) + (2t) &= (2) + (2t) \\
 (t + 1)x^2 &= 2t + 2 && \# \text{ multiply with the multiplicative invers of } t + 1 \\
 (t + 2)(t + 1)x^2 &= (t + 2)(2t + 2) && \# \text{ multiply with the multiplicative invers of } t + 1 \\
 x^2 &= 2 && \# 2 \text{ is quadratic residue. Take the roots.} \\
 x &\in \{t, 2t\}
 \end{aligned}$$

2505 Computations in extension fields are arguably on the edge of what can reasonably be done with  
 2506 pen and paper. Fortunately, Sage provides us with a simple way to do the computations.

```

2507 sage: Z3 = GF(3) # prime field 213
2508 sage: Z3t.<t> = Z3[] # polynomials over Z3 214
2509 sage: P = Z3t(t^2+1) 215
2510 sage: P.is_irreducible() 216
2511 True 217
2512 sage: F3_2.<t> = GF(3^2, name='t', modulus=P) 218
2513 sage: F3_2 219
2514 Finite Field in t of size 3^2 220
2515 sage: F3_2(t+2)*F3_2(2*t+2) == F3_2(2) 221
2516 True 222
2517 sage: F3_2(2*t+2)^(-1) # multiplicative inverse 223
2518 2*t + 1 224

```

```

2519 sage: # verify our solution to (t+1)(x^2 + (2t+2)) = 2      225
2520 sage: F3_2(t+1)*(F3_2(t)**2 + F3_2(2*t+2)) == F3_2(2)      226
2521 True                                                         227
2522 sage: F3_2(t+1)*(F3_2(2*t)**2 + F3_2(2*t+2)) == F3_2(2)      228
2523 True                                                         229

```

2524 *Exercise 44.* Consider the extension field  $\mathbb{F}_{32}$  from the previous example and find all pairs of  
 2525 elements  $(x, y) \in \mathbb{F}_{32}$ , for which the following equation holds:

$$y^2 = x^3 + 4 \quad (4.40)$$

2526 *Exercise 45.* Show that the polynomial  $P = x^3 + x + 1$  from  $\mathbb{F}_5[x]$  is irreducible. Then consider  
 2527 the extension field  $\mathbb{F}_{5^3}$  defined relative to  $P$ . Compute the multiplicative inverse of  $(2t^2 + 4) \in$   
 2528  $\mathbb{F}_{5^3}$  using the extended Euclidean algorithm. Then find all  $x \in \mathbb{F}_{5^3}$  that solve the following  
 2529 equation:

$$(2t^2 + 4)(x - (t^2 + 4t + 2)) = (2t + 3) \quad (4.41)$$

2530 **Hashing into extension fields** On page 66, we have seen how to hash into prime fields. As  
 2531 elements of extension fields can be seen as polynomials over prime fields, hashing into extension  
 2532 fields is therefore possible if every coefficient of the polynomial is hashed independently.

check  
reference

## 2533 4.4 Projective Planes

2534 Projective planes are particular geometric constructs defined over a given field. In a sense,  
 2535 projective planes extend the concept of the ordinary Euclidean plane by including “points at  
 2536 infinity.”

2537 Such an inclusion of infinity points makes projective planes particularly useful in the de-  
 2538 scription of elliptic curves, as the description of such a curve in an ordinary plane needs an  
 2539 additional symbol “the point at infinity” to give the set of points on the curve the structure of  
 2540 a group. Translating the curve into projective geometry includes this “point at infinity” more  
 2541 naturally into the set of all points on a projective plane.

2542 To understand the idea of constructing of projective planes, note that in an ordinary Eu-  
 2543 clidean plane, two lines either intersect in a single point or are parallel. In the latter case, both  
 2544 lines are either the same, that is, they intersect in all points, or do not intersect at all. A projec-  
 2545 tive plane can then be thought of as an ordinary plane, but equipped with additional “point at  
 2546 infinity” such that two different lines always intersect in a single point. Parallel lines intersect  
 2547 “at infinity”.

2548 To be more precise, let  $\mathbb{F}$  be a field,  $\mathbb{F}^3 := \mathbb{F} \times \mathbb{F} \times \mathbb{F}$  the set of all three tuples over  $\mathbb{F}$  and  
 2549  $x \in \mathbb{F}^3$  with  $x = (X, Y, Z)$ . Then there is exactly one *line* in  $\mathbb{F}^3$  that intersects both  $(0, 0, 0)$  and  
 2550  $x$ . This line is given as follows:

$$[X : Y : Z] := \{(k \cdot X, k \cdot Y, k \cdot Z) \mid k \in \mathbb{F}\} \quad (4.42)$$

2551 A **point** in the **projective plane** over  $\mathbb{F}$  is defined as such a **line**, and the projective plane is the  
 2552 set of all such points:

$$\mathbb{FP}^2 := \{[X : Y : Z] \mid (X, Y, Z) \in \mathbb{F}^3 \text{ with } (X, Y, Z) \neq (0, 0, 0)\} \quad (4.43)$$

2553 It can be shown that a projective plane over a finite field  $\mathbb{F}_{p^m}$  contains  $p^{2m} + p^m + 1$  number of  
 2554 elements.

To understand why  $[X : Y : Z]$  is called a line, consider the situation where the underlying field  $\mathbb{F}$  is the set of real numbers  $\mathbb{R}$ . In this case,  $\mathbb{R}^3$  can be seen as the three-dimensional space, and  $[X : Y : Z]$  is an ordinary line in this 3-dimensional space that intersects zero and the point with coordinates  $X$ ,  $Y$  and  $Z$ .

The key observation here is that points in the projective plane are lines in the 3-dimensional space  $\mathbb{F}^3$ . Additionally, for finite fields, the terms **space** and **line** share very little visual similarity with their counterparts over the set of real numbers.

It follows from this that points  $[X : Y : Z] \in \mathbb{F}\mathbb{P}^2$  are not simply described by fixed coordinates  $(X, Y, Z)$ , but by **sets of coordinates**, where two different coordinates  $(X_1, Y_1, Z_1)$  and  $(X_2, Y_2, Z_2)$  describe the same point if and only if there is some field element  $k$  such that  $(X_1, Y_1, Z_1) = (k \cdot X_2, k \cdot Y_2, k \cdot Z_2)$ . Points  $[X : Y : Z]$  are called **projective coordinates**.

*Notation and Symbols* 8 (Projective coordinates). Projective coordinates of the form  $[X : Y : 1]$  are descriptions of so-called **affine points**. Projective coordinates of the form  $[X : Y : 0]$  are descriptions of so-called **points at infinity**. In particular, the projective coordinate  $[1 : 0 : 0]$  describes the so-called **line at infinity**.

*Example 67.* Consider the field  $\mathbb{F}_3$  from example XXX. As this field only contains three elements, it does not take too much effort to construct its associated projective plane  $\mathbb{F}_3\mathbb{P}^2$ , as we know that it only contains 13 elements.

To find  $\mathbb{F}_3\mathbb{P}^2$ , we have to compute the set of all lines in  $\mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3$  that intersect  $(0, 0, 0)$ .

add reference

Since those lines are parameterized by tuples  $(x_1, x_2, x_3)$ , we compute as follows:

$$\begin{aligned}
[0 : 0 : 1] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(0, 0, 1), (0, 0, 2)\} \\
[0 : 0 : 2] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(0, 0, 2), (0, 0, 1)\} = [0 : 0 : 1] \\
[0 : 1 : 0] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(0, 1, 0), (0, 2, 0)\} \\
[0 : 1 : 1] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(0, 1, 1), (0, 2, 2)\} \\
[0 : 1 : 2] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(0, 1, 2), (0, 2, 1)\} \\
[0 : 2 : 0] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(0, 2, 0), (0, 1, 0)\} = [0 : 1 : 0] \\
[0 : 2 : 1] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(0, 2, 1), (0, 1, 2)\} = [0 : 1 : 2] \\
[0 : 2 : 2] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(0, 2, 2), (0, 1, 1)\} = [0 : 1 : 1] \\
[1 : 0 : 0] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(1, 0, 0), (2, 0, 0)\} \\
[1 : 0 : 1] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(1, 0, 1), (2, 0, 2)\} \\
[1 : 0 : 2] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(1, 0, 2), (2, 0, 1)\} \\
[1 : 1 : 0] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(1, 1, 0), (2, 2, 0)\} \\
[1 : 1 : 1] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(1, 1, 1), (2, 2, 2)\} \\
[1 : 1 : 2] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(1, 1, 2), (2, 2, 1)\} \\
[1 : 2 : 0] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(1, 2, 0), (2, 1, 0)\} \\
[1 : 2 : 1] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(1, 2, 1), (2, 1, 2)\} \\
[1 : 2 : 2] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(1, 2, 2), (2, 1, 1)\} \\
[2 : 0 : 0] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(2, 0, 0), (1, 0, 0)\} = [1 : 0 : 0] \\
[2 : 0 : 1] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(2, 0, 1), (1, 0, 2)\} = [1 : 0 : 2] \\
[2 : 0 : 2] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(2, 0, 2), (1, 0, 1)\} = [1 : 0 : 1] \\
[2 : 1 : 0] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(2, 1, 0), (1, 2, 0)\} = [1 : 2 : 0] \\
[2 : 1 : 1] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(2, 1, 1), (1, 2, 2)\} = [1 : 2 : 2] \\
[2 : 1 : 2] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(2, 1, 2), (1, 2, 1)\} = [1 : 2 : 1] \\
[2 : 2 : 0] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(2, 2, 0), (1, 1, 0)\} = [1 : 1 : 0] \\
[2 : 2 : 1] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(2, 2, 1), (1, 1, 2)\} = [1 : 1 : 2] \\
[2 : 2 : 2] &= \{(k \cdot x_1, k \cdot x_2, k \cdot x_3) \mid k \in \mathbb{F}_3\} = \{(2, 2, 2), (1, 1, 1)\} = [1 : 1 : 1]
\end{aligned}$$

These lines define the 13 points in the projective plane  $\mathbb{F}_3\mathbb{P}$ :

$$\begin{aligned}
\mathbb{F}_3\mathbb{P} = \{ & [0 : 0 : 1], [0 : 1 : 0], [0 : 1 : 1], [0 : 1 : 2], [1 : 0 : 0], [1 : 0 : 1], \\
& [1 : 0 : 2], [1 : 1 : 0], [1 : 1 : 1], [1 : 1 : 2], [1 : 2 : 0], [1 : 2 : 1], [1 : 2 : 2] \}
\end{aligned}$$

2573 This projective plane contains 9 affine points, three points at infinity and one line at infinity.

2574 To understand the ambiguity in projective coordinates a bit better, let us consider the point  
 2575  $[1 : 2 : 2]$ . As this point in the projective plane is a line in  $\mathbb{F}_3^3$ , it has the projective coordinates  
 2576  $(1, 2, 2)$  as well as  $(2, 1, 1)$ , since the former coordinate gives the latter when multiplied in  $\mathbb{F}_3$   
 2577 by the factor 2. In addition, note that, for the same reasons, the points  $[1 : 2 : 2]$  and  $[2 : 1 : 1]$   
 2578 are the same, since their underlying sets are equal.

2579 *Exercise 46.* Construct the so-called **Fano plane**, that is, the projective plane over the finite  
 2580 field  $\mathbb{F}_2$ .

# Chapter 5

## Elliptic Curves

Generally speaking, elliptic curves are “curves” defined in geometric planes like the Euclidean or the projective plane over some given field. One of the key features of elliptic curves over finite fields from the point of view of cryptography is that their set of points has a group law such that the resulting group is finite and cyclic, and it is believed that the discrete logarithm problem on these groups is hard.

A special class of elliptic curves are so-called **pairing-friendly curves**, which have a notation of a group pairing as defined in XXX. This pairing has cryptographically advantageous properties. Those curve are useful in the development of SNARKs, since they allow to compute so-called RICS-satisfiability “in the exponent” **MIRCO: (THIS HAS TO BE REWRITTEN WITH WAY MORE DETAIL)**

In this chapter, we introduce epileptic curves as they are used in pairing-based approaches to the construction of SNARKs. The elliptic curves we consider are all defined over prime fields or prime field extensions and the reader should be familiar with the contend of the previous section on those fields.

In its most generality elliptic curves are defined as a smooth projective curve of genus 1 defined over some field  $\mathbb{F}$  with a distinguished  $\mathbb{F}$ -rational point, but this definition is not very useful for the introductory character of this book. We will therefore look at 3 more practical definitions in the following sections, by introducing Weierstraß, Montgomery and Edwards curves. All of them are widely used in cryptography, and understanding them is crucial to being able to follow the rest of this book.

### 5.1 Elliptic Curve Arithmetics

#### 5.1.1 Short Weierstraß Curves

In this section, we introduce **short Weierstraß** curves, which are the most general types of curves over finite fields of characteristic greater than 3.

We start with their representation in **affine space**. This representation has the advantage that affine points correspond to pairs of numbers, which makes it more accessible for beginners. However, it has the disadvantage that a special “point at infinity”, that is not a point on the curve, is necessary to describe the group structure. We introduce the elliptic curve group law and describe elliptic curve scalar multiplication, which is an instantiation of the exponential map from general cyclic groups.

Then we look at the projective representation of short Weierstraß curves. This has the advantage that no special symbol is necessary to represent the point at infinity but comes with

TODO:  
Elliptic  
Curve  
asymmet-  
ric cryp-  
tography  
examples.  
Private  
key, gen-  
erator,  
public  
key.

add refer-  
ence

maybe re-  
move this  
sentence?

affine  
space

the drawback that projective points are classes of numbers, which might be a bit unusual for a beginner.

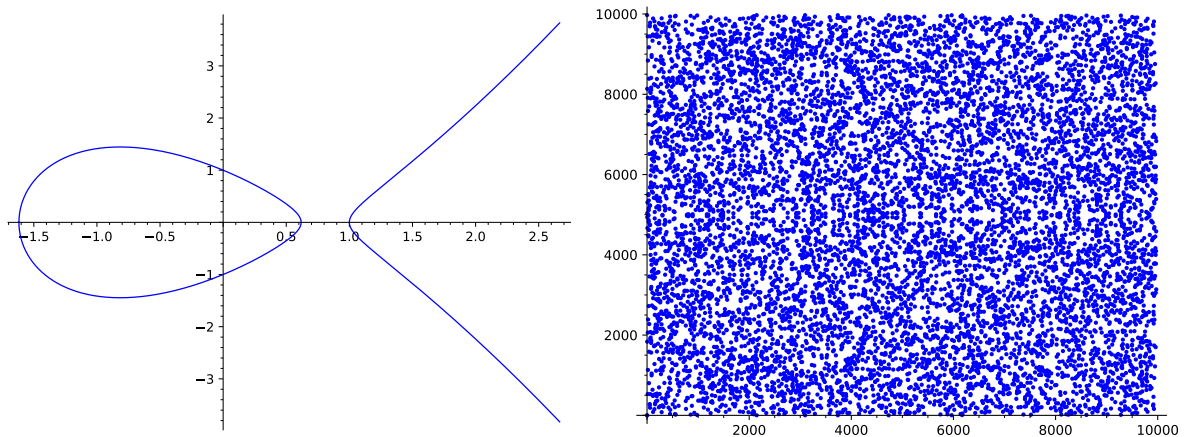
We finish this section with an explicit equivalence that transforms affine representations into projective ones and vice versa.

**Affine short Weierstraß form** Probably the least abstract and most straight-forward way to introduce elliptic curves for non-mathematicians and beginners is the so-called affine representation of a short Weierstraß curve. To see what this is, let  $\mathbb{F}$  be a finite field of order  $q$  and  $a, b \in \mathbb{F}$  two field elements such that  $4a^3 + 27b^2 \bmod q \neq 0$ . Then a **short Weierstraß elliptic curve**  $E(\mathbb{F})$  over  $\mathbb{F}$  in its affine representation is the set of all pairs of field elements  $(x, y) \in \mathbb{F} \times \mathbb{F}$  that satisfy the short Weierstraß cubic equation  $y^2 = x^3 + a \cdot x + b$ , together with a distinguished symbol  $\mathcal{O}$ , called the **point at infinity**:

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid y^2 = x^3 + a \cdot x + b\} \cup \{\mathcal{O}\} \quad (5.1)$$

*Notation and Symbols 9.* In the literature, the set  $E(\mathbb{F})$ , which includes the symbol  $\mathcal{O}$ , is often called the set of **rational points** of the elliptic curve, in which case the curve itself is usually written as  $E/\mathbb{F}$ . However, in what follows, we will frequently identify an elliptic curve with its set of rational points and therefore use the notation  $E(\mathbb{F})$  instead. This is possible in our case, since we only the group structure of the curve in consideration is relevant for us.

The term “curve” is used here because, in the ordinary 2 dimensional plane  $\mathbb{R}^2$ , the set of all points  $(x, y)$  that satisfy  $y^2 = x^3 + a \cdot x + b$  looks like a curve. We should note however that visualizing elliptic curves over finite fields as “curves” has its limitations, and we will therefore not stress the geometric picture too much, but focus on the computational properties instead. To understand the visual difference, consider the following two elliptic curves:



Both elliptic curves are defined by the same short Weierstraß equation  $y^2 = x^3 - 2x + 1$ , but the first curve is defined in the real affine plane  $\mathbb{R}^2$ , that is, the pair  $(x, y)$  contains real numbers, while the second one is defined in the affine plane  $\mathbb{F}_{9973}^2$ , which means that both  $x$  and  $y$  are from the prime field  $\mathbb{F}_{9973}$ . Every blue dot represents a pair  $(x, y)$ , that is a solution to  $y^2 = x^3 - 2x + 1$ . As we can see, the second curve hardly looks like a geometric structure one would naturally call a curve. This shows that our geometric intuitions from  $\mathbb{R}^2$  are obfuscated in curves over finite fields.

The identity  $6 \cdot (4a^3 + 27b^2) \bmod q \neq 0$  ensures that the curve is non-singular, which basically means that the curve has no **cusps** or **self-intersections**.

cusps

self-intersections

Throughout this book, the reader is advised to do as many computations in a pen-and-paper fashion as possible, as this helps getting a deeper understanding of the details. However, when dealing with elliptic curves, computations can quickly become cumbersome and tedious, and one might get lost in the details. Fortunately, Sage is very helpful in dealing with elliptic curves. This book introduces the reader to the great elliptic curve capabilities of Sage. The following snippet shows a way to define elliptic curves and work with them in Sage:

```

sage: F5 = GF(5) # define the base field
sage: a = F5(2) # parameter a
sage: b = F5(4) # parameter b
sage: # check non-singularity
sage: F5(6)*(F5(4)*a^3+F5(27)*b^2) != F5(0)
True
sage: # short Weierstrass curve
sage: E = EllipticCurve(F5,[a,b]) # y^2 == x^3 + ax +b
sage: P = E(0,2) # 2^2 == 0^3 + 2*0 + 4
sage: P.xy() # affine coordinates
(0, 2)
sage: INF = E(0) # point at infinity
sage: try: # point at infinity has no affine coordinates
.....:     INF.xy()
.....: except ZeroDivisionError:
.....:     pass
sage: P = E.plot() # create a plotted version

```

The following three examples give a more practical understanding of what an elliptic curve is and how we can compute it. The reader is advised to read them carefully, and ideally, to also carry out the computation themselves. We will repeatedly build on these examples in this chapter, and use the second example throughout this book.

*Example 68.* To provide the reader with an example of a small elliptic curve where all computation can be done with pen and paper, consider the prime field  $\mathbb{F}_5$  from example 62 (page 64), which should be quite familiar to readers who had worked through the examples and exercises in the previous chapter.

To define an elliptic curve over  $\mathbb{F}_5$ , we have to choose two numbers  $a$  and  $b$  from that field. Assuming we choose  $a = 1$  and  $b = 1$  then  $4a^3 + 27b^2 \equiv 1 \pmod{5}$  from which follows that the corresponding elliptic curve  $E_1(\mathbb{F}_5)$  is given by the set of all pairs  $(x, y)$  from  $\mathbb{F}_5$  that satisfy the equation  $y^2 = x^3 + x + 1$ , together with the special symbol  $\mathcal{O}$ , which represents the “point at infinity”.

To get a better understanding of that curve, observe that if we choose arbitrarily the pair  $(x, y) = (1, 1)$ , we see that  $1^2 \neq 1^3 + 1 + 1$  and hence  $(1, 1)$  is not an element of the curve  $E_1(\mathbb{F}_5)$ . On the other hand choosing for example  $(x, y) = (2, 1)$  gives  $1^2 = 2^3 + 2 + 1$  and hence the pair  $(2, 1)$  is an element of  $E_1(\mathbb{F}_5)$  (Remember that all computations are done in modulo 5 arithmetics).

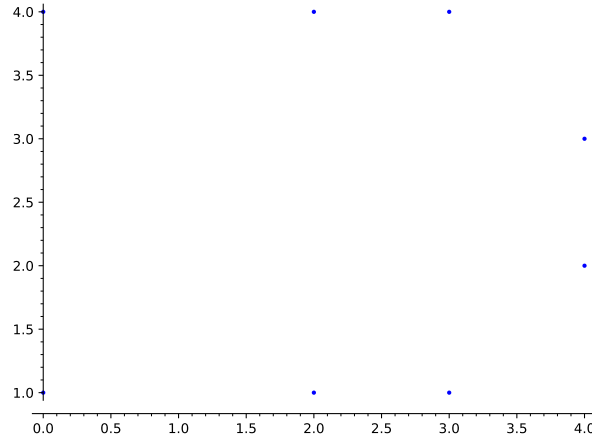
Now since the set  $\mathbb{F}_5 \times \mathbb{F}_5$  of all pairs  $(x, y)$  from  $\mathbb{F}_5$  contains only  $5 \cdot 5 = 25$  pairs, we can compute the curve, by just inserting every possible pair  $(x, y)$  into the short Weierstraß equation  $y^2 = x^3 + x + 1$ . If the equation holds, the pair is a curve point, if not that means that the point is not on the curve. Combining the result of this computation with the point at infinity gives the curve as follows:

$$E_1(\mathbb{F}_5) = \{\mathcal{O}, (0, 1), (2, 1), (3, 1), (4, 2), (4, 3), (0, 4), (2, 4), (3, 4)\}$$

check  
reference



2687 This means that our elliptic curve is a set of 9 elements, 8 of which are pairs of numbers and  
 2688 one special symbol  $\mathcal{O}$ . Visualizing  $E_1$  gives the following plot:



2690 In the development of SNARKs, it is sometimes necessary to do elliptic curve cryptography  
 2691 “in a circuit”, which basically means that the elliptic curves need to be implemented in a certain  
 2692 SNARK-friendly way. We will look at what this means in chapter 7. [To be able to do this](#)  
 2693 efficiently, it is desirable to have curves with special properties. The following example is a  
 2694 pen-and-paper version of such a curve, called **Baby-jubjub**, which resembles cryptographically  
 2695 secure curves extensively used in real-world SNARKs. The interested reader is advised to study  
 2696 this example carefully, as we will use it and build on it in various places throughout the book. S:  
 2697 I feel like a lot of people won’t get the Lewis Carroll reference unless we make it more explicit.  
 2698 M: The term Baby-JubJub is actually the name of a curve used in zCash and Ethereum a lot.  
 2699 IDK why they choosed that name.

check  
reference

jubjub

2700 *Example 69* (Tiny-Jubjub). Consider the prime field  $\mathbb{F}_{13}$  from exercise 4.3.1 (page 66. [If we](#)  
 2701 choose  $a = 8$  and  $b = 8$ , then  $4a^3 + 27b^2 \equiv 6 \pmod{13}$  and the corresponding elliptic curve  
 2702 is given by all pairs  $(x, y)$  from  $\mathbb{F}_{13}$  such that  $y^2 = x^3 + 8x + 8$  holds. We call this curve the  
 2703 **Tiny-jubjub** curve, or *TJJ\_13* for short.

check  
reference

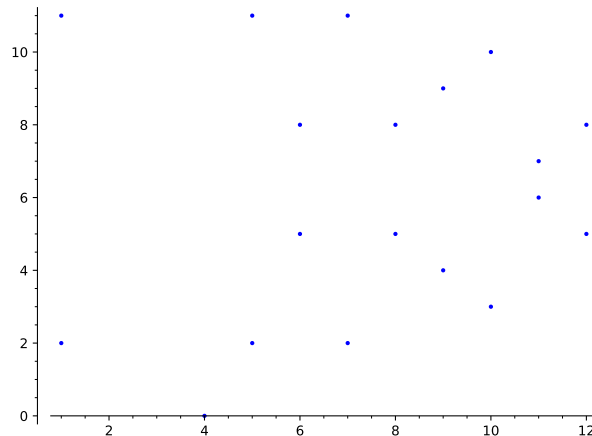
2704 Now, since the set  $\mathbb{F}_{13} \times \mathbb{F}_{13}$  of all pairs  $(x, y)$  from  $\mathbb{F}_{13}$  contains only  $13 \cdot 13 = 169$  pairs,  
 2705 we can compute the curve by just inserting every possible pair  $(x, y)$  into the short Weierstraß  
 2706 equation  $y^2 = x^3 + 8x + 8$ . We get the following result:

$$\begin{aligned} TJJ_{13} = \{ \mathcal{O}, (1, 2), (1, 11), (4, 0), (5, 2), (5, 11), (6, 5), (6, 8), (7, 2), (7, 11), (8, 5), (8, 8), \\ (9, 4), (9, 9), (10, 3), (10, 10), (11, 6), (11, 7), (12, 5), (12, 8) \} \end{aligned} \quad (5.2)$$

2707 As we can see, the curve consists of 20 points; 19 points from the [affine plane](#) and the point at  
 2708 infinity. To get a visual impression of the *TJJ\_13* curve, we might plot all of its points (except  
 2709 the point at infinity) in the  $\mathbb{F}_{13} \times \mathbb{F}_{13}$  affine plane. We get the following plot:

affine  
plane





2710

2711 As we will see in what follows, this curve is rather special, as it is possible to represent it in two  
 2712 alternative forms called the **Montgomery** and the **twisted Edwards form** (See sections 5.1.2  
 2713 and 5.1.3, respectively).

check  
reference

2714 Now that we have seen two pen-and-paper friendly elliptic curves, let us look at a curve, that  
 2715 is used in actual cryptography. Cryptographically secure elliptic curves are not **qualitatively**  
 2716 different from the curves we looked at so far, but the prime number modulus of their prime field  
 2717 is much larger. Typical examples use prime numbers that have binary representations in the  
 2718 magnitude of more than double the size of the desired security level. If, for example, a security  
 2719 of 128 bits is desired, a prime modulus of binary size  $\geq 256$  is chosen. The following example  
 2720 provides such a curve.

check  
reference

*Example 70* (Bitcoin's Secp256k1 curve). To give an example of a real-world, cryptographically secure curve, let us look at curve Secp256k1, which is famous for being used in the public key cryptography of Bitcoin. The prime field  $\mathbb{F}_p$  of Secp256k1 is defined by the following prime number:

$$p = 115792089237316195423570985008687907853269984665640564039457584007908834671663$$

2721 The binary representation of this number needs 256 bits, which implies that the prime field  
 2722  $\mathbb{F}_p$  contains approximately  $2^{256}$  many elements, which is considered quite large. To get a better  
 2723 impression of how large the base field is, consider that the number  $2^{256}$  is approximately in the  
 2724 same order of magnitude as the estimated number of atoms in the observable universe.

The curve Secp256k1 is defined by the parameters  $a, b \in \mathbb{F}_p$  with  $a = 0$  and  $b = 7$ . Since  $4 \cdot 0^3 + 27 \cdot 7^2 \bmod p = 1323$ , those parameters indeed define an elliptic curve given as follows:

$$\text{Secp256k1} = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + 7\}$$

Clearly, the Secp256k1 curve is too large to do computations by hand, since it can be shown that the number of its elements is a prime number  $r$  that also has a binary representation of 256 bits:

$$r = 115792089237316195423570985008687907852837564279074904382605163141518161494337$$

2725 Cryptographically secure elliptic curves are therefore not useful in pen-and-paper computations.  
 2726 Fortunately, Sage handles large curves efficiently:

2727 **sage:** `p = 1157920892373161954235709850086879078532699846656405` 247  
 2728 `64039457584007908834671663`

```

2729 sage: # Hexadecimal representation
2730 sage: p.str(16)
2731 ffffffffffffffffffffffffffffffffffffffffffffffffffefffffc
2732 2f
2733 sage: p.is_prime()
2734 True
2735 sage: p.nbits()
2736 256
2737 sage: Fp = GF(p)
2738 sage: Secp256k1 = EllipticCurve(Fp, [0, 7])
2739 sage: r = Secp256k1.order() # number of elements
2740 sage: r.str(16)
2741 fffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd03641
2742 41
2743 sage: r.is_prime()
2744 True
2745 sage: r.nbits()
2746 256

```

2747 *Exercise 47.* Look up the definition of curve BLS12-381, implement it in Sage and compute its  
 2748 order.

2749 **Affine compressed representation** As we have seen in example 70, cryptographically secure  
 2750 elliptic curves are defined over large prime fields, where elements of those fields typically need  
 2751 more than 255 bits of storage on a computer. Since elliptic curve points consist of pairs of those  
 2752 field elements, they need double that amount of storage.

2753 However, we can reduce the amount of space needed to represent a curve point by using  
 2754 a technique called **point compression**. Note that, up to a sign, the y coordinate of a curve  
 2755 point can be computed from the  $x$  coordinate by simply inserting  $x$  into the Weierstraß equation  
 2756 and then computing the roots of the result. This gives two results, and it means that we can  
 2757 represent a curve point in **compressed form** by simply storing the  $x$  coordinate together with  
 2758 a single sign bit only, the latter of which deterministically decides which of the two roots to  
 2759 choose. One convention could be to always choose the root closer to 0 when the sign bit is 0,  
 2760 and the root closer to the order of  $\mathbb{F}$  when the sign bit is 1. In case the  $y$  coordinate is zero, both  
 2761 sign bits give the same result.

*Example 71* (Tiny-jubjub). To understand the concept of compressed curve points a bit better,  
 consider the *TJJ\_13* curve from example 69 again. Since this curve is defined over the prime  
 field  $\mathbb{F}_{13}$ , and numbers between 0 and 13 need approximately 4 bits to be represented, each  
*TJJ\_13* point on this curve needs 8 bits of storage in uncompressed form. The following set  
 represents the uncompressed form of the points on this curve:

$$TJJ\_13 = \{\mathcal{O}, (1, 2), (1, 11), (4, 0), (5, 2), (5, 11), (6, 5), (6, 8), (7, 2), (7, 11), \\ (8, 5), (8, 8), (9, 4), (9, 9), (10, 3), (10, 10), (11, 6), (11, 7), (12, 5), (12, 8)\}$$

Using the technique of point compression, we can reduce the bits needed to represent the points  
 on this curve to 5 per point. To achieve this, we can replace the  $y$  coordinate in each  $(x, y)$  pair  
 by a sign bit indicating whether or not  $y$  is closer to 0 or to 13. As a result  $y$  values in the range  
 $[0, \dots, 6]$  will have the sign bit 0, while  $y$ -values in the range  $[7, \dots, 12]$  will have the sign bit 1.

check  
reference

sign

more ex-  
planation  
of what  
the sign is

check  
reference

Applying this to the points in *TJJ\_13* gives the compressed representation as follows:

$$TJJ_{13} = \{\mathcal{O}, (1,0), (1,1), (4,0), (5,0), (5,1), (6,0), (6,1), (7,0), (7,1), \\ (8,0), (8,1), (9,0), (9,1), (10,0), (10,1), (11,0), (11,1), (12,0), (12,1)\}$$

Note that the numbers  $7, \dots, 12$  are the negatives (additive inverses) of the numbers  $1, \dots, 6$  in modular 13 arithmetics and that  $-0 = 0$ . Calling the compression bit a “sign bit” therefore makes sense.

To recover the uncompressed counterpart of, say, the compressed point  $(5, 1)$ , we insert the  $x$  coordinate 5 into the Weierstraß equation and get  $y^2 = 5^3 + 8 \cdot 5 + 8 = 4$ . As expected, 4 is a quadratic residue in  $\mathbb{F}_{13}$  with roots  $\sqrt{4} = \{2, 11\}$ . Since the sign bit of the point is 1, we have to choose the root closer to the modulus 13, which is 11. The uncompressed point is therefore  $(5, 11)$ .

Looking at the previous examples, the compression rate does not look very impressive. However, looking at the real-life example of the Secp256k1 curve shows that compression is has significant practical advantages.

*Example 72.* Consider the Secp256k1 curve from example 70 again. The following code invokes Sage to generate a random affine curve point, then applies our compression method to it:

```
sage: P = Secp256k1.random_point().xy()
sage: P
(1821895723447173372882423257921269223458531419923781212435813
 5196816791153162, 10544428255723937879936207898085010105914
 1336383605667210928086595288446317114)
sage: # uncompressed affine point size
sage: ZZ(P[0]).nbits()+ZZ(P[1]).nbits()
510
sage: # compute the compression
sage: if P[1] > Fp(-1)/Fp(2):
.....:     PARITY = 1
.....: else:
.....:     PARITY = 0
sage: PCOMPRESSED = [P[0], PARITY]
sage: PCOMPRESSED
[1821895723447173372882423257921269223458531419923781212435813
 5196816791153162, 1]
sage: # compressed affine point size
sage: ZZ(PCOMPRESSED[0]).nbits()+ZZ(PCOMPRESSED[1]).nbits()
255
```

**Affine group law** One of the key properties of an elliptic curve is that it is possible to define a group law on the set of its rational points such that the point at infinity serves as the neutral element and inverses are reflections on the  $x$ -axis.

The origin of this law can be understood in a geometric picture and is known as the **chord-and-tangent rule**. In the affine representation of a short Weierstraß curve, the rule can be described in the following way:

S: I don't follow this at all

check reference

add explanation of how this shows what we claim

**Definition 5.1.1.1. Chord-and-tangent rule**

- (Point at infinity) We define the point at infinity  $\mathcal{O}$  as the neutral element of addition, that is, we define  $P + \mathcal{O} = P$  for all points  $P \in E(\mathbb{F})$ .
- (Point addition) Let  $P, Q \in E(\mathbb{F}) \setminus \{\mathcal{O}\}$  with  $P \neq Q$  be two distinct points on an elliptic curve, neither of them the point at infinity. The sum of  $P$  and  $Q$  is defined as follows: Consider the line  $l$  which intersects the curve in  $P$  and  $Q$ . If  $l$  intersects the elliptic curve at a third point  $R'$ , define the sum  $R = P \oplus Q$  of  $P$  and  $Q$  as the reflection of  $R'$  at the  $x$ -axis. If the line  $l$  does not intersect the curve at a third point, define the sum to be the point at infinity  $\mathcal{O}$ . It can be shown that no such **chord line** will intersect the curve in more than three points, so addition is not ambiguous.
- (Point doubling) Let  $P \in E(\mathbb{F}) \setminus \{\mathcal{O}\}$  be a point on an elliptic curve, that is not the point at infinity. The sum of  $P$  with itself (the doubling of  $P$ ) is defined as follows: Consider the line which is **tangential** to the elliptic curve at  $P$ . If this line intersects the elliptic curve at a second point  $R'$ , the sum  $2P = P + P$  is the reflection of  $R'$  at the  $x$ -axis. If it does not intersect the curve at a third, point define the sum to be the point at infinity  $\mathcal{O}$ . It can be shown that no such **tangent line** will intersect the curve in more than two points, so addition is not ambiguous.

It can be shown that the points of an elliptic curve form a commutative group with respect to the tangent-and-chord rule such that  $\mathcal{O}$  acts the neutral element, and the inverse of any element  $P \in E(\mathbb{F})$  is the reflection of  $P$  on the  $x$ -axis.

To translate the geometric description into algebraic equations, first observe that, for any two given curve points  $(x_1, y_1), (x_2, y_2) \in E(\mathbb{F})$ , it can be shown that the identity  $x_1 = x_2$  implies  $y_2 = \pm y_1$ , which shows that the following rules are a complete description of the affine addition law.

**Definition 5.1.1.2. Chord-and-tangent rule: algebraic equations**

- (Neutral element) The point at infinity  $\mathcal{O}$  is the neutral element.
- (Additive inverse ) The additive inverse of  $\mathcal{O}$  is  $\mathcal{O}$ . For any other curve point  $(x, y) \in E(\mathbb{F}) \setminus \{\mathcal{O}\}$ , the additive inverse is given by  $(x, -y)$ .
- (Addition rule) For any two curve points  $P, Q \in E(\mathbb{F})$ , addition is defined by one of the following three cases:
  1. (Adding the neutral element) If  $Q = \mathcal{O}$ , then the sum is defined as  $P \oplus Q = P$ .
  2. (Adding inverse elements) If  $P = (x, y)$  and  $Q = (x, -y)$ , the sum is defined as  $P \oplus Q = \mathcal{O}$ .
  3. (Adding non-self-inverse equal points) If  $P = (x, y)$  and  $Q = (x, y)$  with  $y \neq 0$ , the sum  $2P = (x', y')$  is defined as follows: **We only referred to  $P$  in the definition of point doubling above so  $Q$  seems a bit confusing here even though it's defined as equal to  $P$**
  4. (Adding non-inverse different points) If  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$  such that  $x_1 \neq x_2$ , the sum  $R = P + Q$  with  $R = (x_3, y_3)$  is defined as follows:

$$x' = \left( \frac{3x^2 + a}{2y} \right)^2 - 2x \quad , \quad y' = \left( \frac{3x^2 + a}{2y} \right)^2 (x - x') - y$$

$$x_3 = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \quad , \quad y_3 = \left( \frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) - y_1$$

2836 Note that short Weierstraß curve points  $P$  with  $P = (x, 0)$  are inverses of themselves, which  
 2837 implies  $2P = \mathcal{O}$  in this case.

2838 *Notation and Symbols 10.* Let  $\mathbb{F}$  be a field and  $E(\mathbb{F})$  be an elliptic curve over  $\mathbb{F}$ . We write  $\oplus$  for  
 2839 the group law on  $E(\mathbb{F})$  and  $(E(\mathbb{F}), \oplus)$  for the group of rational points.

2840 As we can see, it is very efficient to compute inverses on elliptic curves. However, com-  
 2841 puting the addition of elliptic curve points in the affine representation needs to consider many  
 2842 cases and involves extensive finite field divisions. As we will see in the next paragraph, this can  
 2843 be simplified in projective coordinates. where?

2844 To get some practical impression of how the group law on an elliptic curve is computed,  
 2845 let's look at some actual cases:

*Example 73.* Consider the elliptic curve  $E_1(\mathbb{F}_5)$  from example 68 again. As we have seen, the  
 set of rational points contains 9 elements: check  
reference

$$E_1(\mathbb{F}_5) = \{\mathcal{O}, (0, 1), (2, 1), (3, 1), (4, 2), (4, 3), (0, 4), (2, 4), (3, 4)\}$$

2846 We know that this set defines a group, so we can add any two elements from  $E_1(\mathbb{F}_5)$  to get a  
 2847 third element.

To give an example, consider the elements  $(0, 1)$  and  $(4, 2)$ . Neither of these elements is  
 the neutral element  $\mathcal{O}$ , and since, the  $x$  coordinate of  $(0, 1)$  is different from the  $x$  coordinate of  
 $(4, 2)$ , we know that we have to use the chord rule, that is, rule number 4 from definition 5.1.1.2,  
 to compute the sum  $(0, 1) \oplus (4, 2)$ : check  
reference

$$\begin{aligned} x_3 &= \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 && \# \text{ insert points} \\ &= \left( \frac{2 - 1}{4 - 0} \right)^2 - 0 - 4 && \# \text{ simplify in } \mathbb{F}_5 \\ &= \left( \frac{1}{4} \right)^2 + 1 = 4^2 + 1 = 1 + 1 = 2 \end{aligned}$$

$$\begin{aligned} y_3 &= \left( \frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) - y_1 && \# \text{ insert points} \\ &= \left( \frac{2 - 1}{4 - 0} \right) (0 - 2) - 1 && \# \text{ simplify in } \mathbb{F}_5 \\ &= \left( \frac{1}{4} \right) \cdot 3 + 4 = 4 \cdot 3 + 4 = 2 + 4 = 1 \end{aligned}$$

So, in our elliptic curve  $E_1(\mathbb{F}_5)$  we get  $(0, 1) \oplus (4, 2) = (2, 1)$ , and, indeed, the pair  $(2, 1)$  is an  
 element of  $E_1(\mathbb{F}_5)$  as expected. On the other hand,  $(0, 1) \oplus (0, 4) = \mathcal{O}$ , since both points have  
 equal  $x$  coordinates and inverse  $y$  coordinates, rendering them inverses of each other. Adding  
 the point  $(4, 2)$  to itself, we have to use the tangent rule, that is, rule 3 from definition 5.1.1.2: check  
reference

$$\begin{aligned}
 x' &= \left( \frac{3x^2 + a}{2y} \right)^2 - 2x && \# \text{ insert points} \\
 &= \left( \frac{3 \cdot 4^2 + 1}{2 \cdot 2} \right)^2 - 2 \cdot 4 && \# \text{ simplify in } \mathbb{F}_5 \\
 &= \left( \frac{3 \cdot 1 + 1}{4} \right)^2 + 3 \cdot 4 = \left( \frac{4}{4} \right)^2 + 2 = 1 + 2 = 3
 \end{aligned}$$

$$\begin{aligned}
 y' &= \left( \frac{3x^2 + a}{2y} \right)^2 (x - x') - y && \# \text{ insert points} \\
 &= \left( \frac{3 \cdot 4^2 + 1}{2 \cdot 2} \right)^2 (4 - 3) - 2 && \# \text{ simplify in } \mathbb{F}_5 \\
 &= 1 \cdot 1 + 3 = 4
 \end{aligned}$$

2848 So, in our elliptic curve  $E_1(\mathbb{F}_5)$ , we get the doubling of  $(4, 2)$ , that is,  $(4, 2) \oplus (4, 2) = (3, 4)$ ,  
 2849 and, indeed the pair  $(3, 4)$  is an element of  $E_1(\mathbb{F}_5)$  as expected. The group  $E_1(\mathbb{F}_5)$  has no self-  
 2850 inverse points other than the neutral element  $\mathcal{O}$ , since no point has 0 as its y coordinate. We can  
 2851 invoke Sage to double-check the computations.

```

2852 sage: F5 = GF(5)                                281
2853 sage: E1 = EllipticCurve(F5, [1, 1])             282
2854 sage: INF = E1(0) # point at infinity             283
2855 sage: P1 = E1(0, 1)                               284
2856 sage: P2 = E1(4, 2)                               285
2857 sage: P3 = E1(0, 4)                               286
2858 sage: R1 = E1(2, 1)                               287
2859 sage: R2 = E1(3, 4)                               288
2860 sage: R1 == P1+P2                                 289
2861 True                                              290
2862 sage: INF == P1+P3                                291
2863 True                                              292
2864 sage: R2 == P2+P2                                 293
2865 True                                              294
2866 sage: R2 == 2*P2                                  295
2867 True                                              296
2868 sage: P3 == P3 + INF                              297
2869 True                                              298

```

*Example 74* (Tiny-jubjub). Consider the *TJJ\_13*-curve from example 69 again and recall that its group of rational points is given as follows:

check  
reference

$$\begin{aligned}
 TJJ_{13} = \{ &\mathcal{O}, (1, 2), (1, 11), (4, 0), (5, 2), (5, 11), (6, 5), (6, 8), (7, 2), (7, 11), \\
 &(8, 5), (8, 8), (9, 4), (9, 9), (10, 3), (10, 10), (11, 6), (11, 7), (12, 5), (12, 8) \}
 \end{aligned}$$

2870 In contrast to the group from the previous example, this group contains a self-inverse point,  
 2871 which is different from the neutral element, defined by  $(4, 0)$ . To see what this means, observe  
 2872 that we cannot add  $(4, 0)$  to itself using the tangent rule 3 from definition 5.1.1.2, as the y  
 2873 coordinate is zero. Instead, we have to use rule 2, since  $0 = -0$ . We therefore get  $(4, 0) \oplus$

check  
reference

2874  $(4,0) = \mathcal{O}$  in *TJJ\_13*. The point  $(4,0)$  is therefore the inverse of itself, as adding it to itself  
 2875 results in the neutral element.

```

2876 sage: F13 = GF(13)                                     299
2877 sage: MJJ = EllipticCurve(F13, [8, 8])                  300
2878 sage: P = MJJ(4, 0)                                     301
2879 sage: INF = MJJ(0) # Point at infinity                  302
2880 sage: INF == P+P                                         303
2881 True                                                    304
2882 sage: INF == 2*P                                         305
2883 True                                                    306

```

2884 *Example 75.* Consider the Secp256k1 curve from example 70 again. The following code in-  
 2885 vokes Sage to generate a random affine curve point, then applies our compression method:

check  
reference

```

2886 sage: P = Secp256k1.random_point()                      307
2887 sage: Q = Secp256k1.random_point()                      308
2888 sage: INF = Secp256k1(0)                                309
2889 sage: R1 = -P                                           310
2890 sage: R2 = P + Q                                         311
2891 sage: R3 = Secp256k1.order()*P                          312
2892 sage: P.xy()                                             313
2893 (3061525366938856869152295649989583106526562933430970836396736 314
2894      8897302545632990, 99215820851053288134824177630971362022838
2895      335784563689240650400137404459232955)
2896 sage: Q.xy()                                             315
2897 (4137686487398629387139788761156282790874390637734876215639041 316
2898      9976451231853782, 82497993246331995439214386723057701561358
2899      72836762668696002093544332262775651)
2900 sage: (ZZ(R1[0]).str(16), ZZ(R1[1]).str(16))            317
2901 ('43af9e98274ce833ddb4a7651c0e2e12bf83198bce1e4871d314da4b2871 318
2902      0ede', '24a5d5de89a7e8815843cf585fdc85b93475431c38dd6bb6a28
2903      1e9234ef44d74')
2904 sage: R2.xy()                                             319
2905 (4379930589901896442985835532818390568198262794372571022326716 320
2906      9609335391597014, 72689167127674314522882623686216427948034
2907      829218297591913418269174751655730940)
2908 sage: R3 == INF                                           321
2909 True                                                    322
2910 sage: P[1]+R1[1] == Fp(0) # -(x,y) = (x,-y)           323
2911 True                                                    324

```

2912 *Exercise 48.* Consider the *TJJ\_13*-curve from example 69.

check  
reference

- 2913 1. Compute the inverse of  $(10,10)$ ,  $\mathcal{O}$ ,  $(4,0)$  and  $(1,2)$ .
- 2914 2. Compute the expression  $3 \cdot (1,11) - (9,9)$ .
- 2915 3. Solve the equation  $x + 2(9,4) = (5,2)$  for some  $x \in TJJ_{13}$
- 2916 4. Solve the equation  $x \cdot (7,11) = (8,5)$  for  $x \in \mathbb{Z}$



**Scalar multiplication** As we have seen in the previous section, elliptic curves  $E(\mathbb{F})$  have the structure of a commutative group associated to them. Moreover, It can moreover be shown that this group is finite and cyclic whenever the field is finite.

To understand elliptic curve scalar multiplication, recall from page 43 that every finite cyclic group of order  $q$  has a generator  $g$  and an associated exponential map  $g^{(\cdot)} : \mathbb{Z}_q \rightarrow \mathbb{G}$ , where  $g^n$  is the  $n$ -fold product of  $g$  with itself.

check  
reference

Elliptic curve scalar multiplication is the exponential map written in additive notation. To be more precise, let  $\mathbb{F}$  be a finite field,  $E(\mathbb{F})$  an elliptic curve of order  $r$ , and  $P$  a generator of  $E(\mathbb{F})$ . Then the **elliptic curve scalar multiplication** with base  $P$  is defined as follows (where  $[0]P = \mathcal{O}$  and  $[m]P = P + P + \dots + P$  is the  $m$ -fold sum of  $P$  with itself):

$$[\cdot]P : \mathbb{Z}_r \rightarrow E(\mathbb{F}); m \mapsto [m]P$$

therefore, elliptic curve scalar multiplication is an instantiation of the general exponential map using additive instead of multiplicative notation. This map is a homomorph of groups, which means that  $[n + m]P = [n]P \oplus [m]P$ .

As with all finite, cyclic groups, the inverse of the exponential map exists and is usually called the **elliptic curve discrete logarithm map**. However, elliptic curves are believed to be XXX-groups, which means that we don't know of any efficient way to actually compute this map.

add term

Scalar multiplication and its inverse, the elliptic curve discrete logarithm, define the **elliptic curve discrete logarithm problem**, which consists of finding solutions  $m \in \mathbb{Z}_r$  such that the following equation holds:

$$P = [m]Q \quad (5.3)$$

Any solution  $m$  is usually called a **discrete logarithm relation** between  $P$  and  $Q$ . If  $Q$  is a generator of the curve, then there is a discrete logarithm relation between  $Q$  and any other point, since  $Q$  generates the group by repeatedly adding  $Q$  to itself. Therefore, we know that some discrete logarithm relation exists for generator  $Q$  and point  $P$ . However, since elliptic curves are believed to be XXX-groups, finding actual relations  $m$  is computationally hard, with runtimes being approximately the size of the order of the group. In practice, we often need the assumption that a discrete logarithm relation exists, while the relation itself is not known.

add term

One useful property of the exponential map in regard to the examples in this book is that it can be used to greatly simplify pen-and-paper computations. As we have seen in example XXX, computing the elliptic curve addition law takes quite a bit of effort when done without a computer. However, when  $g$  is a generator of a small pen-and-paper elliptic curve group of order  $r$ , we can use the exponential map to write the group using cofactor clearing, which implies that  $[r]g = \mathcal{O}$ :

add refer-  
encecofactor  
clearing

$$\mathbb{G} = \{[1]g \rightarrow [2]g \rightarrow [3]g \rightarrow \dots \rightarrow [r-1]g \rightarrow \mathcal{O}\} \quad (5.4)$$

“Logarithmic ordering” like this greatly simplifies complicated elliptic curve addition to the much simpler case of modular  $r$  addition. In order to add two curve points  $P$  and  $Q$ , we only have to look up their discrete log relations with the generator, say  $P = [n]g$  and  $Q = [m]g$ , and compute the sum as  $P \oplus Q = [n + m]g$ . This is, of course, only possible for small groups where we can keep a clear overview, such as XXX.

add refer-  
ence

In the following example, we will look at some implications of the fact that elliptic curves are finite cyclic groups. We will apply the fundamental theorem of finite cyclic groups and look how it reflects on the curves in consideration.

*Example 76.* Consider the elliptic curve group  $E_1(\mathbb{F}_5)$  from example 68. Since it is a finite cyclic group of order 9, and the prime factorization of 9 is  $3 \cdot 3$ , we can use the fundamental

check  
reference



theorem of finite cyclic groups to reason about all its subgroups. In fact, since the only prime factor of 9 is 3, we know that  $E_1(\mathbb{F}_5)$  has the following subgroups:

- $\mathbb{G}_1 = E_1(\mathbb{F}_5)$  is a subgroup of order 9. By definition, any group is a subgroup of itself.
- $\mathbb{G}_2 = \{(2, 1), (2, 4), \mathcal{O}\}$  is a subgroup of order 3. This is the subgroup associated to the prime factor 3.
- $\mathbb{G}_3 = \{\mathcal{O}\}$  is a subgroup of order 1. This is the trivial subgroup.

Moreover, since  $E_1(\mathbb{F}_5)$  and all its subgroups are cyclic, we know from page 43 that they must have generators. For example, the curve point  $(2, 1)$  is a generator of the order 3 subgroup  $\mathbb{G}_2$ , since every element of  $\mathbb{G}_2$  can be generated by repeatedly adding  $(2, 1)$  to itself:

check  
reference

$$\begin{aligned}[1](2, 1) &= (2, 1) \\ [2](2, 1) &= (2, 4) \\ [3](2, 1) &= \mathcal{O}\end{aligned}$$

Since  $(2, 1)$  is a generator, we know from XXX that it gives rise to an exponential map from the finite field  $\mathbb{F}_3$  onto  $\mathbb{G}_2$  defined by scalar multiplication:

add refer-  
ence

$$[\cdot](2, 1) : \mathbb{F}_3 \rightarrow \mathbb{G}_2 : x \mapsto [x](2, 1)$$

To give an example of a generator that generates the entire group  $E_1(\mathbb{F}_5)$ , consider the point  $(0, 1)$ . Applying the tangent rule repeatedly, we compute as follows:

$$\begin{array}{ll} [0](0, 1) = \mathcal{O} & [1](0, 1) = (0, 1) \\ [2](0, 1) = (4, 2) & [3](0, 1) = (2, 1) \\ [4](0, 1) = (3, 4) & [5](0, 1) = (3, 1) \\ [6](0, 1) = (2, 4) & [7](0, 1) = (4, 3) \\ [8](0, 1) = (0, 4) & [9](0, 1) = \mathcal{O} \end{array}$$

Again, since  $(2, 1)$  is a generator, we know from XXX that it gives rise to an exponential map. However, since the group order is not a prime number, the exponential map does not map from any field, but from the residue class ring  $\mathbb{Z}_9$  only:

add refer-  
ence

$$[\cdot](0, 1) : \mathbb{Z}_9 \rightarrow \mathbb{G}_1 : x \mapsto [x](0, 1)$$

Using the generator  $(0, 1)$  and its associated exponential map, we can write  $E(\mathbb{F}_1)$  i logarithmic order with respect to  $(0, 1)$  as explained in equation 5.4. We get the following:

check  
reference

$$E_1(\mathbb{F}_5) = \{(0, 1) \rightarrow (4, 2) \rightarrow (2, 1) \rightarrow (3, 4) \rightarrow (3, 1) \rightarrow (2, 4) \rightarrow (4, 3) \rightarrow (0, 4) \rightarrow \mathcal{O}\}$$

This indicates that the first element is a generator, and the  $n$ -th element is the scalar product of  $n$  and the generator. To see how logarithmic orders like this simplify the computations in small elliptic curve groups, consider example 73 again. In that example, we use the chord-and-tangent rule to compute  $(0, 1) \oplus (4, 2)$ . Now, in the logarithmic order of  $E_1(\mathbb{F})$ , we can compute that sum much easier, since we can directly see that  $(0, 1) = [1](0, 1)$  and  $(4, 2) = [2](0, 1)$ . We can then deduce  $(0, 1) \oplus (4, 2) = (2, 1)$  immediately, since  $[1](0, 1) \oplus [2](0, 1) = [3](0, 1) = (2, 1)$ .

check  
reference

To give another example, we can immediately see that  $(3, 4) \oplus (4, 3) = (4, 2)$ , without doing any expensive elliptic curve addition, since we know  $(3, 4) = [4](0, 1)$  as well as  $(4, 3) =$

2970  $[7](0, 1)$  from the logarithmic representation of  $E_1(\mathbb{F}_5)$ . Since  $4 + 7 = 2$  in  $\mathbb{Z}_9$ , the result must  
 2971 be  $[2](0, 1) = (4, 2)$ .

2972 Finally we can use  $E_1(\mathbb{F}_5)$  as an example to understand the concept of cofactor clearing from  
 2973 5.4. Since the order of  $E_1(\mathbb{F}_5)$  is 9, we only have a single factor, which happen to be the cofactor  
 2974 as well. Cofactor clearing then implies that we can map any element from  $E_1(\mathbb{F}_5)$  onto its prime  
 2975 factor group  $\mathbb{G}_2$  by scalar multiplication with 3. For example, taking the element  $(3, 4)$ , which  
 2976 is not in  $\mathbb{G}_2$ , and multiplying it with 3, we get  $[3](3, 4) = (2, 1)$ , which is an element of  $\mathbb{G}_2$  as  
 2977 expected.

check  
reference

2978 In the following example, we will look at the subgroups of our tiny-jubjub curve, define  
 2979 generators, and compute the logarithmic order for pen-and-paper computations. Then we take  
 2980 another look at the principle of cofactor clearing.

2981 *Example 77.* Consider the tiny-jubjub curve  $TJJ\_13$  from example 69 again. Since the order of  
 2982  $TJJ\_13$  is 20, and the prime factorization of 20 is  $2^2 \cdot 5$ , we know that the  $TJJ\_13$  contains a  
 2983 “large” prime-order subgroup of size 5 and a small prime order subgroup of size 2.

check  
reference

2984 To compute those groups, we can apply the technique of cofactor clearing in a try-and-repeat  
 2985 loop. We start the loop by arbitrarily choosing an element  $P \in TJJ\_13$ , then multiplying that  
 2986 element with the cofactor of the group that we want to compute. If the result is  $\mathcal{O}$ , we try a  
 2987 different element and repeat the process until the result is different from the point at infinity  $\mathcal{O}$ .

2988 To compute a generator for the small prime-order subgroup  $(TJJ\_13)_2$ , first observe that the  
 2989 cofactor is 10, since  $20 = 2 \cdot 10$ . We then arbitrarily choose the curve point  $(5, 11) \in TJJ\_13$   
 2990 and compute  $[10](5, 11) = \mathcal{O}$ . Since the result is the point at infinity, we have to try another  
 2991 curve point, say  $(9, 4)$ . We get  $[10](9, 4) = (4, 0)$  and we can deduce that  $(4, 0)$  is a generator  
 2992 of  $(TJJ\_13)_2$ . Logarithmic order then gives  $(TJJ\_13)_2 = \{(4, 0) \rightarrow \mathcal{O}\}$  as expected, since we  
 2993 know from example 74 that  $(4, 0)$  is self-inverse, with  $(4, 0) \oplus (4, 0) = \mathcal{O}$ . We double check the  
 2994 computations using Sage:

check  
reference

2995	<b>sage:</b> <code>F13 = GF(13)</code>	325
2996	<b>sage:</b> <code>TJJ = EllipticCurve(F13, [8, 8])</code>	326
2997	<b>sage:</b> <code>P = TJJ(5, 11)</code>	327
2998	<b>sage:</b> <code>INF = TJJ(0)</code>	328
2999	<b>sage:</b> <code>10*P == INF</code>	329
3000	<b>True</b>	330
3001	<b>sage:</b> <code>Q = TJJ(9, 4)</code>	331
3002	<b>sage:</b> <code>R = TJJ(4, 0)</code>	332
3003	<b>sage:</b> <code>10*Q == R</code>	333
3004	<b>True</b>	334

We can apply the same reasoning to the “large” prime-order subgroup  $(TJJ\_13)_5$ , which contains 5 elements. To compute a generator for this group, first observe that the associated cofactor is 4, since  $20 = 5 \cdot 4$ . We choose the curve point  $(9, 4) \in TJJ\_13$  again, and compute  $[4](9, 4) = (7, 11)$ . We can deduce that  $(7, 11)$  is a generator of  $(TJJ\_13)_5$ . Using the generator  $(7, 11)$ , we compute the exponential map  $[\cdot](7, 11) : \mathbb{F}_5 \rightarrow TJJ\_13$  and get the following:

Explain  
how

$$\begin{aligned}
 [0](7, 11) &= \mathcal{O} \\
 [1](7, 11) &= (7, 11) \\
 [2](7, 11) &= (8, 5) \\
 [3](7, 11) &= (8, 8) \\
 [4](7, 11) &= (7, 2)
 \end{aligned}$$

We can use this computation to write the large-order prime group  $(TJJ\_13)_5$  of the tiny-jubjub curve in logarithmic order, which we will use quite frequently in what follows. We get the following:

$$(TJJ\_13)_5 = \{(7, 11) \rightarrow (8, 5) \rightarrow (8, 8) \rightarrow (7, 2) \rightarrow \mathcal{O}\} \quad (5.5)$$

From this, we can immediately see, for example that  $(8, 8) \oplus (7, 2) = (8, 5)$ , since  $3 + 4 = 2$  in  $\mathbb{F}_5$ .

From the previous two examples, the reader might get the impression that elliptic curve computation can be largely replaced by modular arithmetics. This however, is not true in general, but only an artifact of small groups, where it is possible to write the entire group in a logarithmic order. The following example gives some understanding of why this is not possible in cryptographically secure groups.

*Example 78.* SEKTP BICOIN. DISCRETE LOG HARDNESS PROHIBITS ADDITION IN THE FIELD...

write example

**Projective short Weierstraß form** As we have seen in the previous section, describing elliptic curves as pairs of points that satisfy a certain equation is relatively straight-forward. However, in order to define a group structure on the set of points, we had to add a special point at infinity to act as the neutral element.

Recalling from the definition of projective planes (section 4.4), we know that points at infinity are handled as ordinary points in projective geometry. Therefore, it makes sense to look at the definition of a short Weierstraß curve in projective geometry.

check reference

To see what a short Weierstraß curve in projective coordinates is, let  $\mathbb{F}$  be a finite field of order  $q$  and characteristic  $> 3$ , let  $a, b \in \mathbb{F}$  be two field elements such that  $4a^3 + 27b^2 \bmod q \neq 0$  and let  $\mathbb{FP}^2$  be the projective plane over  $\mathbb{F}$ . Then a **short Weierstraß elliptic curve** over  $\mathbb{F}$  in its projective representation is the set of all points  $[X : Y : Z] \in \mathbb{FP}^2$  from the projective plane that satisfy the **homogenous** cubic equation  $Y^2 \cdot Z = X^3 + a \cdot X \cdot Z^2 + b \cdot Z^3$ :

$$E(\mathbb{FP}^2) = \{[X : Y : Z] \in \mathbb{FP}^2 \mid Y^2 \cdot Z = X^3 + a \cdot X \cdot Z^2 + b \cdot Z^3\} \quad (5.6)$$

To understand how the point at infinity is unified in this definition, recall from XXX that, in projective geometry, points at infinity are given by homogeneous coordinates  $[X : Y : 0]$ . Inserting representatives  $(x_1, y_1, 0) \in [X : Y : 0]$  from those classes into the defining homogenous cubic equations gives the following:

add reference

$$\begin{aligned} y_1^2 \cdot 0 &= x_1^3 + a \cdot x_1 \cdot 0^2 + b \cdot 0^3 \\ 0 &= x_1^3 \end{aligned} \quad \Leftrightarrow$$

This shows that the only point at infinity, that is also a point on a projective short Weierstraß curve is the class  $[0, 1, 0] = \{(0, y, 0) \mid y \in \mathbb{F}\}$ .

This point is the projective representation of  $\mathcal{O}$ . The projective representation of a short Weierstraß curve, therefore, has the advantage that it does not need a special symbol to represent the point at infinity  $\mathcal{O}$  from the affine definition.

*Example 79.* To get an intuition of how an elliptic curve in projective geometry looks, consider curve  $E_1(\mathbb{F}_5)$  from example (68). We know that, in its affine representation, the set of rational points is given as follows:

check reference

$$E_1(\mathbb{F}_5) = \{\mathcal{O}, (0, 1), (2, 1), (3, 1), (4, 2), (4, 3), (0, 4), (2, 4), (3, 4)\} \quad (5.7)$$

3037 This is defined as the set of all pairs  $(x, y) \in \mathbb{F}_5 \times \mathbb{F}_5$  such that the affine short Weierstraß  
 3038 equation  $y^2 = x^3 + ax + b$  with  $a = 1$  and  $b = 1$  is satisfied.

3039 To find the projective representation of a short Weierstraß curve with the same parameters  
 3040  $a = 1$  and  $b = 1$ , we have to compute the set of projective points  $[X : Y : Z]$  from the projec-  
 3041 tive plane  $\mathbb{F}_5\mathbb{P}^2$  that satisfy the following homogenous cubic equation for any representative  
 3042  $(x_1, y_1, z_1) \in [X : Y : Z]$ :

$$y_1^2 z_1 = x_1^3 + 1 \cdot x_1 z_1^2 + 1 \cdot z_1^3 \quad (5.8)$$

3043 We know from XXX that the projective plane  $\mathbb{F}_5\mathbb{P}^2$  contains  $5^2 + 5 + 1 = 31$  elements, so we  
 3044 can take the effort and insert all elements into equation 5.8 and see if both sides match.

For example, consider the projective point  $[0 : 4 : 1]$ . We know from XXX that this point in  
 the projective plane represents the following line in the three-dimensional space  $\mathbb{F}^3$ :

$$[0 : 4 : 1] = \{(0, 0, 0), (0, 4, 1), (0, 3, 2), (0, 2, 3), (0, 1, 4)\}$$

To check whether or not  $[0 : 4 : 1]$  satisfies 5.8, we can insert any representative, in other words,  
 any element from XXX. Each element satisfies the equation if and only if all other elements  
 satisfy the equation. So, we insert  $(0, 4, 1)$  and get the following result:

$$1^2 \cdot 1 = 0^3 + 1 \cdot 0 \cdot 1^2 + 1 \cdot 1^3$$

This tells us that the affine point  $[0 : 4 : 1]$  is indeed a solution to the equation 5.8, but we  
 could just as well have inserted any other representative. For example, inserting  $(0, 3, 2)$  also  
 satisfies 5.8:

$$3^2 \cdot 2 = 0^3 + 1 \cdot 0 \cdot 2^2 + 1 \cdot 2^3$$

3045 To find the projective representation of  $E_1$ , we first observe that the projective line at infinity  
 3046  $[1 : 0 : 0]$  is not a curve point on any projective short Weierstraß curve, since it cannot satisfy  
 3047 XXX for any parameter  $a$  and  $b$ . Therefore, we can exclude it from our consideration.

3048 Moreover, a point at infinity  $[X : Y : 0]$  can only satisfy equation XXX for any  $a$  and  $b$ , if  
 3049  $X = 0$ , which implies that the only point at infinity relevant for short Weierstraß elliptic curves  
 3050 is  $[0 : 1 : 0]$ , since  $[0 : k : 0] = [0 : 1 : 0]$  for all  $k$  from the finite field. Therefore, we can exclude  
 3051 all points at infinity except the point  $[0 : 1 : 0]$ .

3052 All points that remain are the affine points  $[X : Y : 1]$ . Inserting all of them into XXX, we  
 3053 get the set of all projective curve points as follows:

$$E_1(\mathbb{F}_5\mathbb{P}^2) = \{[0 : 1 : 0], [0 : 1 : 1], [2 : 1 : 1], [3 : 1 : 1], \\ [4 : 2 : 1], [4 : 3 : 1], [0 : 4 : 1], [2 : 4 : 1], [3 : 4 : 1]\}$$

3054 If we compare this with the affine representation, we see that there is a 1:1 correspondence  
 3055 between the points in the affine representation in 5.7 and the affine points in projective geometry,  
 3056 and that the point  $[0 : 1 : 0]$  represents the additional point  $\mathcal{O}$  in the projective representation.

3057 *Exercise 49.* Compute the projective representation of the tiny-jubjub curve and the logarithmic  
 3058 order of its large prime-order subgroup with respect to the generator  $(7, 11)$ .

3059 **Projective Group law** As we have seen on page 73, one of the key properties of an elliptic  
 3060 curve is that it comes with a definition of a group law on the set of its rational points, described  
 3061 geometrically by the chord-and-tangent rule (definition 5.1.1.1). This rule was kind of intuitive,

with the exception of the distinguished point at infinity, which appeared whenever the chord or the tangent did not have a third intersection point with the curve.

One of the key features of projective coordinates is that, in projective space, it is guaranteed that any chord will always intersect the curve in three points, and any tangent will intersect it in two points including the tangent point. So, the geometric picture simplifies, as we don't need to consider external symbols and associated cases.

Again, it can be shown that the points of an elliptic curve in projective space form a commutative group with respect to the tangent-and-chord rule such that the projective point  $[0 : 1 : 0]$  is the neutral element, and the additive inverse of a point  $[X : Y : Z]$  is given by  $[X : -Y : Z]$ . The addition law is usually described by the following algorithm, minimizing the number of necessary additions and multiplications in the base field.

*Exercise 50.* Compare the affine addition law for short Weierstraß curves with the projective addition rule. Which branch in the projective rule corresponds to which case in the affine law?

Check if following Alg is floated too far

**Coordinate Transformations** As we have seen in example XXX, there was a close relation between the affine and the projective representation of a short Weierstraß curve. This was not a coincidence. In fact, from a mathematical point of view, projective and affine short Weierstraß curves describe the same thing, as there is a one-to-one correspondence (an isomorphism) between both representations for any arbitrary parameters  $a$  and  $b$ .

add reference

To specify the isomorphism, let  $E(\mathbb{F})$  and  $E(\mathbb{FP}^2)$  be an affine and a projective short Weierstraß curve defined for the same parameters  $a$  and  $b$ . Then the map in 5.9 maps points from the affine representation to points from the projective representation of a short Weierstraß curve. In other words, if the pair of points  $(x, y)$  satisfies the affine equation  $y^2 = x^3 + ax + b$ , then all homogeneous coordinates  $(x_1, y_1, z_1) \in [x : y : 1]$  satisfy the projective equation  $y_1^2 \cdot z_1 = x_1^3 + ay_1 \cdot z_1^2 + b \cdot z_1^3$ .

$$\Phi : E(\mathbb{F}) \rightarrow E(\mathbb{FP}^2) : \begin{array}{ll} (x, y) & \mapsto [x : y : 1] \\ \mathcal{O} & \mapsto [0 : 1 : 0] \end{array} \quad (5.9)$$

The inverse is given by the following map:

$$\Phi^{-1} : E(\mathbb{FP}^2) \rightarrow E(\mathbb{F}) : [X : Y : Z] \mapsto \begin{cases} (\frac{X}{Z}, \frac{Y}{Z}) & \text{if } Z \neq 0 \\ \mathcal{O} & \text{if } Z = 0 \end{cases} \quad (5.10)$$

Note that the only projective point  $[X : Y : Z]$  with  $Z \neq 0$  that satisfies XXX is given by the class  $[0 : 1 : 0]$ .

add reference

One key feature of  $\Phi$  and its inverse is that it respects the group structure, which means that  $\Phi((x_1, y_1) \oplus (x_2, y_2))$  is equal to  $\Phi(x_1, y_1) \oplus \Phi(x_2, y_2)$ . The same holds true for the inverse map  $\Phi^{-1}$ .

Maps with these properties are called **group isomorphisms**, and, from a mathematical point of view, the existence of  $\Phi$  implies that these two definitions are equivalent, and implementations can choose freely between these representations.

## 5.1.2 Montgomery Curves

History and use of them (optimized scalar multiplication)

write up this part

**Algorithm 6** Projective Weierstraß Addition Law

---

**Require:**  $[X_1 : Y_1 : Z_1], [X_2 : Y_2 : Z_2] \in E(\mathbb{F}_{\mathbb{P}}^2)$

**procedure** ADD-RULE( $[X_1 : Y_1 : Z_1], [X_2 : Y_2 : Z_2]$ )

**if**  $[X_1 : Y_1 : Z_1] == [0 : 1 : 0]$  **then**

$[X_3 : Y_3 : Z_3] \leftarrow [X_2 : Y_2 : Z_2]$

**else if**  $[X_2 : Y_2 : Z_2] == [0 : 1 : 0]$  **then**

$[X_3 : Y_3 : Z_3] \leftarrow [X_1 : Y_1 : Z_1]$

**else**

$U_1 \leftarrow Y_2 \cdot Z_1$

$U_2 \leftarrow Y_1 \cdot Z_2$

$V_1 \leftarrow X_2 \cdot Z_1$

$V_2 \leftarrow X_1 \cdot Z_2$

**if**  $V_1 == V_2$  **then**

**if**  $U_1 \neq U_2$  **then**  $[X_3 : Y_3 : Z_3] \leftarrow [0 : 1 : 0]$

**else**

**if**  $Y_1 == 0$  **then**  $[X_3 : Y_3 : Z_3] \leftarrow [0 : 1 : 0]$

**else**

$W \leftarrow a \cdot Z_1^2 + 3 \cdot X_1^2$

$S \leftarrow Y_1 \cdot Z_1$

$B \leftarrow X_1 \cdot Y_1 \cdot S$

$H \leftarrow W^2 - 8 \cdot B$

$X' \leftarrow 2 \cdot H \cdot S$

$Y' \leftarrow W \cdot (4 \cdot B - H) - 8 \cdot Y_1^2 \cdot S^2$

$Z' \leftarrow 8 \cdot S^3$

$[X_3 : Y_3 : Z_3] \leftarrow [X' : Y' : Z']$

**end if**

**end if**

**else**

$U = U_1 - U_2$

$V = V_1 - V_2$

$W = Z_1 \cdot Z_2$

$A = U^2 \cdot W - V^3 - 2 \cdot V^2 \cdot V_2$

$X' = V \cdot A$

$Y' = U \cdot (V^2 \cdot V_2 - A) - V^3 \cdot U_2$

$Z' = V^3 \cdot W$

$[X_3 : Y_3 : Z_3] \leftarrow [X' : Y' : Z']$

**end if**

**end if**

**return**  $[X_3 : Y_3 : Z_3]$

**end procedure**

**Ensure:**  $[X_3 : Y_3 : Z_3] == [X_1 : Y_1 : Z_1] \oplus [X_2 : Y_2 : Z_2]$

---

**Affine Montgomery Form** To see what a Montgomery curve in affine coordinates is, let  $\mathbb{F}$  be a finite field of characteristic  $> 2$ , and let  $A, B \in \mathbb{F}$  be two field elements such that  $B \neq 0$  and  $A^2 \neq 4$ . A **Montgomery elliptic curve**  $M(\mathbb{F})$  over  $\mathbb{F}$  in its affine representation is the set of all pairs of field elements  $(x, y) \in \mathbb{F} \times \mathbb{F}$  that satisfy the Montgomery cubic equation  $B \cdot y^2 = x^3 + A \cdot x^2 + x$ , together with a distinguished symbol  $\mathcal{O}$ , called the **point at infinity**.

$$M(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid B \cdot y^2 = x^3 + A \cdot x^2 + x\} \cup \{\mathcal{O}\} \quad (5.11)$$

Despite the fact that Montgomery curves look different from short Weierstraß curves, they are just a special way to describe certain short Weierstraß curves. In fact, every curve in affine Montgomery form can be transformed into an elliptic curve in Weierstraß form. To see that, assume that a curve is given in Montgomery form  $By^2 = x^3 + Ax^2 + x$ . The associated Weierstraß form is then as follows:

$$y^2 = x^3 + \frac{3 - A^2}{3B^2} \cdot x + \frac{2A^3 - 9A}{27B^3} \quad (5.12)$$

On the other hand, an elliptic curve  $E(\mathbb{F})$  over base field  $\mathbb{F}$  in Weierstraß form  $y^2 = x^3 + ax + b$  can be converted to Montgomery form if and only if the following conditions hold:

**Definition 5.1.2.1. Requirements for Montgomery curves**

- The number of points on  $E(F)$  is divisible by 4
- The polynomial  $z^3 + az + b \in \mathbb{F}[z]$  has at least one root  $z_0 \in \mathbb{F}$
- $3z_0^2 + a$  is a quadratic residue in  $\mathbb{F}$ .

When these conditions are satisfied, then for  $s = (\sqrt{3z_0^2 + a})^{-1}$ , the equivalent Montgomery curve is defined by the following equation:

$$sy^2 = x^3 + (3z_0s)x^2 + x \quad (5.13)$$

In the following example we will look at our tiny-jubjub curve again, and show that it is actually a Montgomery curve.

**Example 80.** Consider the prime field  $\mathbb{F}_{13}$  and the tiny-jubjub curve  $TJJ\_13$  from example 69. To see that it is a Montgomery curve, we have to check the requirements from 5.1.2.1:

Since the order of  $TJJ\_13$  is 20, which is divisible by 4, the first requirement is met.

Next, since  $a = 8$  and  $b = 8$ , we have to check if the polynomial  $P(z) = z^3 + 8z + 8$  has a root in  $\mathbb{F}_{13}$ . We simply evaluate  $P$  at all numbers  $z \in \mathbb{F}_{13}$ , and find that  $P(4) = 0$ , so a root is given by  $z_0 = 4$ .

In the last step, we have to check that  $3 \cdot z_0^2 + a$  has a root in  $\mathbb{F}_{13}$ . We compute as follows:

$$\begin{aligned} 3z_0^2 + a &= 3 \cdot 4^2 + 8 \\ &= 3 \cdot 3 + 8 \\ &= 9 + 8 \\ &= 4 \end{aligned}$$

To see if 4 is a quadratic residue, we can use Euler's criterion (4.34) to compute the Legendre symbol of 4. We get the following:

is the label in L<sup>A</sup>T<sub>E</sub>X correct here?

check reference

check reference

check reference



$$\left(\frac{4}{13}\right) = 4^{\frac{13-1}{2}} = 4^6 = 1$$

3126 This means that 4 does have a root in  $\mathbb{F}_{13}$ . In fact, computing a root of 4 in  $\mathbb{F}_{13}$  is easy, since  
 3127 the integer root 2 of 4 is also one of its roots in  $\mathbb{F}_{13}$ . The other root is given by  $13 - 4 = 9$ .

Since all requirements are met, we have now shown that *TJJ\_13* is indeed a Montgomery curve, and we can use 5.13 to compute its associated Montgomery form. We compute as follows:

check  
reference

$$\begin{aligned} s &= \left( \sqrt{3 \cdot z_0^2 + 8} \right)^{-1} \\ &= 2^{-1} && \# \text{ Fermat's little theorem} \\ &= 2^{13-2} && \# 2048 \bmod 13 = 7 \\ &= 7 \end{aligned}$$

The defining equation for the Montgomery form of our tiny-jubjub curve is then given by the following equation:

$$\begin{aligned} sy^2 &= x^3 + (3z_0s)x^2 + x && \Rightarrow \\ 7 \cdot y^2 &= x^3 + (3 \cdot 4 \cdot 7)x^2 + x && \Leftrightarrow \\ 7 \cdot y^2 &= x^3 + 6x^2 + x \end{aligned}$$

3128 So, we get the defining parameters as  $B = 7$  and  $A = 6$ , and we can write the tiny-jubjub curve  
 3129 in its affine Montgomery representation as follows:

$$TJJ\_13 = \{(x, y) \in \mathbb{F}_{13} \times \mathbb{F}_{13} \mid 7 \cdot y^2 = x^3 + 6x^2 + x\} \cup \{\mathcal{O}\} \quad (5.14)$$

Now that we have the abstract definition of our tiny-jubjub curve in Montgomery form, we can compute the set of points by inserting all pairs  $(x, y) \in \mathbb{F}_{13} \times \mathbb{F}_{13}$  similarly to how we computed the curve points in its Weierstraß representation. We get the following:

$$TJJ\_13 = \{\mathcal{O}, (0, 0), (1, 4), (1, 9), (2, 4), (2, 9), (3, 5), (3, 8), (4, 4), (4, 9), (5, 1), (5, 12), (7, 1), (7, 12), (8, 1), (8, 12), (9, 2), (9, 11), (10, 3), (10, 10)\}$$

3130

```

3131 sage: F13 = GF(13)                                     335
3132 sage: L_MTJJ = []                                       336
3133 .....: for x in F13:                                    337
3134 .....:     for y in F13:                                338
3135 .....:         if F13(7)*y^2 == x^3 + F13(6)*x^2 + x:  339
3136 .....:             L_MTJJ.append((x, y))                340
3137 sage: MTJJ = Set(L_MTJJ)                                341
3138 sage: # does not compute the point at infinity          342

```

3139 **Affine Montgomery coordinate transformation** Comparing the Montgomery representa-  
 3140 tion of the previous example (equation 5.14) with the Weierstraß representation of the same  
 3141 curve (equation 5.2), we see that there is a 1:1 correspondence between the curve points in both

check  
reference



examples. This is no accident. In fact, if  $M_{A,B}$  is a Montgomery curve, and  $E_{a,b}$  a Weierstraß curve with  $a = \frac{3-A^2}{3B^2}$  and  $b = \frac{2A^2-9A}{27B^3}$  then the following function maps all points in Montgomery representation onto the points in Weierstraß representation:

$$\Phi : M_{A,B} \rightarrow E_{a,b} : (x,y) \mapsto \left( \frac{3x+A}{3B}, \frac{y}{B} \right) \quad (5.15)$$

This map is a 1:1 correspondence (an isomorphism), and its inverse map is given by the following equation (where  $z_0$  is a root of the polynomial  $z^3 + az + b \in \mathbb{F}[z]$  and  $s = (\sqrt{3z_0^2 + a})^{-1}$ ).

$$\Phi^{-1} : E_{a,b} \rightarrow M_{A,B} : (x,y) \mapsto (s \cdot (x - z_0), s \cdot y) \quad (5.16)$$

Using this map, it is therefore possible for implementations of Montgomery curves to freely transit between the Weierstraß and the Montgomery representation. However, as we saw in definition 5.1.2.1, not every Weierstraß curve is a Montgomery curve, as all criteria in 5.1.2.1 have to be satisfied. This means that the map  $\Phi^{-1}$  does not always exist.

*Example 81.* Consider our tiny-jubjub curve again. In equation 5.2 we derived its Weierstraß representation and in example 5.14, we derived its Montgomery representation.

To see how coordinate transformation  $\Phi$  works in this example, let's map points from the Montgomery representation onto points from the Weierstraß representation. Inserting, for example, the point  $(0,0)$  from the Montgomery representation 5.14 into  $\Phi$  gives the following:

$$\begin{aligned} \Phi(0,0) &= \left( \frac{3 \cdot 0 + A}{3B}, \frac{0}{B} \right) \\ &= \left( \frac{3 \cdot 0 + 6}{3 \cdot 7}, \frac{0}{7} \right) \\ &= \left( \frac{6}{8}, 0 \right) \\ &= (4,0) \end{aligned}$$

As we can see, the Montgomery point  $(0,0)$  maps to the self-inverse point  $(4,0)$  of the Weierstraß representation. On the other hand, we can use our computations of  $s = 7$  and  $z_0 = 4$  from XXX to compute the inverse map  $\Phi^{-1}$ , which maps points on the Weierstraß representation to points on the Montgomery form. Inserting, for example,  $(4,0)$  we get the following:

$$\begin{aligned} \Phi^{-1}(4,0) &= (s \cdot (4 - z_0), s \cdot 0) \\ &= (7 \cdot (4 - 4), 0) \\ &= (0,0) \end{aligned}$$

As expected, the inverse map maps the Weierstraß point back to where it originated in the Montgomery form. We can invoke Sage to check that our computation of  $\Phi$  is correct:

```

3155 sage: # Compute PHI of Montgomery form: 343
3156 sage: L_PHI_MTJJ = [] 344
3157 sage: for (x,y) in L_MTJJ: # LMJJ as defined previously 345
3158     . . . . . v = (F13(3)*x + F13(6)) / (F13(3)*F13(7)) 346
3159     . . . . . w = y/F13(7) 347
3160     . . . . . L_PHI_MTJJ.append( (v,w) ) 348

```

check  
reference

check  
reference

check  
reference

check  
reference

check  
reference

add refer-  
ence

```

3161 sage: PHI_MTJJ = Set(L_PHI_MTJJ) 349
3162 sage: # Computation Weierstrass form 350
3163 sage: C_WTJJ = EllipticCurve(F13, [8, 8]) 351
3164 sage: L_WTJJ = [P.xy() for P in C_WTJJ.points() if P.order() > 352
3165 1]
3166 sage: WTJJ = Set(L_WTJJ) 353
3167 sage: # check PHI(Montgomery) == Weierstrass 354
3168 sage: WTJJ == PHI_MTJJ 355
3169 True 356
3170 sage: # check the inverse map PHI^(-1) 357
3171 sage: L_PHIINV_WTJJ = [] 358
3172 sage: for (v,w) in L_WTJJ: 359
3173 .....:     x = F13(7)*(v-F13(4)) 360
3174 .....:     y = F13(7)*w 361
3175 .....:     L_PHIINV_WTJJ.append((x,y)) 362
3176 sage: PHIINV_WTJJ = Set(L_PHIINV_WTJJ) 363
3177 sage: MTJJ == PHIINV_WTJJ 364
3178 True 365

```

3179 **Montgomery group law** We have seen that Montgomery curves special cases of short Weier-  
3180 straß curves. As such, they have a group structure defined on the set of their points, which can  
3181 also be derived from the chord-and-tangent rule. In accordance with short Weierstraß curves, it  
3182 can be shown that the identity  $x_1 = x_2$  implies  $y_2 = \pm y_1$ , meaning that the following rules are a  
3183 complete description of the affine addition law.

3184 *Definition 5.1.2.2. Montgomery group law*

- 3185 • (Neutral element) Point at infinity  $\mathcal{O}$  is the neutral element.
- 3186 • (Additive inverse ) The additive inverse of  $\mathcal{O}$  is  $\mathcal{O}$ . For any other curve point  $(x,y) \in$   
3187  $M(\mathbb{F}_q) \setminus \{\mathcal{O}\}$ , the additive inverse is given by  $(x, -y)$ .
- 3188 • (Addition rule) For any two curve points  $P, Q \in M(\mathbb{F}_q)$ , addition is defined by one of the  
3189 following cases:
  - 3190 1. (Adding the neutral element) If  $Q = \mathcal{O}$ , then the sum is defined as  $P + Q = P$ .
  - 3191 2. (Adding inverse elements) If  $P = (x,y)$  and  $Q = (x, -y)$ , the sum is defined as  $P +$   
3192  $Q = \mathcal{O}$ .
  3. (Adding non-self-inverse equal points) If  $P = (x,y)$  and  $Q = (x,y)$  with  $y \neq 0$ , the  
sum  $2P = (x', y')$  is defined as follows:

$$x' = \left( \frac{3x_1^2 + 2Ax_1 + 1}{2By_1} \right)^2 \cdot B - (x_1 + x_2) - A, \quad y' = \frac{3x_1^2 + 2Ax_1 + 1}{2By_1} (x_1 - x') - y_1$$

4. (Adding non-inverse different points) If  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$  such that  $x_1 \neq$   
 $x_2$ , the sum  $R = P + Q$  with  $R = (x_3, y_3)$  is defined as follows:

$$x' = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 B - (x_1 + x_2) - A, \quad y' = \frac{y_2 - y_1}{x_2 - x_1} (x_1 - x') - y_1$$

### 5.1.3 Twisted Edwards Curves

As we have seen in 5.1.2.2 both Weierstraß and Montgomery curves have somewhat complicated addition and doubling laws, as many cases have to be distinguished. Those various cases translate to branches in computer programs.

check  
reference

In the context of SNARK development, two computational models for bounded computations are used, called **circuits** and **rank-1 constraint systems**. Program branches are undesirably costly when implemented in those models. It is therefore advantageous to look for curves with an addition/doubling rule that requires no branches and as few field operations as possible.

**Twisted Edwards curves** are particularly useful here, as a subclass of these curves has a compact and easily implementable addition law that works for all points including the point at infinity. Implementing this law needs no branching.

**Twisted Edwards Form** To see what an affine **twisted Edwards curve** looks like, let  $\mathbb{F}$  be a finite field of characteristic  $> 2$ , and let  $a, d \in \mathbb{F} \setminus \{0\}$  be two non-zero field elements with  $a \neq d$ . A **twisted Edwards elliptic curve** in its affine representation is the set of all pairs  $(x, y)$  from  $\mathbb{F} \times \mathbb{F}$  that satisfy the twisted Edwards equation  $a \cdot x^2 + y^2 = 1 + d \cdot x^2 y^2$ , given below:

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid a \cdot x^2 + y^2 = 1 + d \cdot x^2 y^2\} \quad (5.17)$$

A twisted Edwards curve is called an **Edwards curve (non-twisted)**, if the parameter  $a$  is equal to 1, and it is called a **SNARK-friendly twisted Edwards curve** if the parameter  $a$  is a quadratic residue and the parameter  $d$  is a quadratic non-residue.

As we can see from the definition, affine twisted Edwards curves look somewhat different from Weierstraß curves, as their affine representation does not need a special symbol to represent the point at infinity. In fact, we will see that the pair  $(0, 1)$  is always a point on any twisted Edwards curve, and that it takes the role of the point at infinity.

Despite their different appearances however, twisted Edwards curves are equivalent to Montgomery curves in the sense that, for every twisted Edwards curve, there is a Montgomery curve, and a way to map the points of one curve in a 1:1 correspondence onto the other and vice versa. To see that, assume that a curve in twisted Edwards form  $a \cdot x^2 + y^2 = 1 + d \cdot x^2 y^2$  is given. The associated Montgomery curve is then defined by the Montgomery equation:

$$\frac{4}{a-d} y^2 = x^3 + \frac{2(a+d)}{a-d} \cdot x^2 + x \quad (5.18)$$

On the other hand, a Montgomery curve  $By^2 = x^3 + Ax^2 + x$  with  $B \neq 0$  and  $A^2 \neq 4$  can give rise to a twisted Edwards curve defined by the following equation:

$$\left(\frac{A+2}{B}\right)x^2 + y^2 = 1 + \left(\frac{A-2}{B}\right)x^2 y^2 \quad (5.19)$$

As we have seen in equation 5.12 and the following discussion, **Montgomery curves are just a special class of Weierstraß curves**. Furthermore we now know that twisted Edwards curves are special Weierstraß curves too. This means that the more general way to describe elliptic curves is as Weierstraß curves.

check  
reference

*Example 82.* Consider the tiny-jubjub curve from example 69 again. We know from example 80 that it is a **Montgomery curve**, and, since **Montgomery curves are equivalent to twisted Edwards curves**, we want to write this curve in twisted Edwards form. We use equation 5.19,

check  
reference

check  
reference

check  
reference

and compute the parameters  $a$  and  $d$  as follows:

$$\begin{aligned}
 a &= \frac{A+2}{B} && \# \text{ insert } A=6 \text{ and } B=7 \\
 &= \frac{8}{7} = 3 && \# 7^{-1} = 2 \\
 \\ 
 d &= \frac{A-2}{B} \\
 &= \frac{4}{7} = 8
 \end{aligned}$$

Thus, we get the defining parameters as  $a = 3$  and  $d = 8$ . Since our goal is to use this curve later on in implementations of pen-and-paper SNARKs, let us show that tiny-jubjub is also a **SNARK-friendly** twisted Edwards curve. To see that, we have to show that  $a$  is a quadratic residue and  $d$  is a quadratic non-residue. We therefore compute the Legendre symbols of  $a$  and  $d$  using Euler's criterion. We get the following:

$$\begin{aligned}
 \left( \frac{3}{13} \right) &= 3^{\frac{13-1}{2}} \\
 &= 3^6 = 1
 \end{aligned}$$

$$\begin{aligned}
 \left( \frac{8}{13} \right) &= 8^{\frac{13-1}{2}} \\
 &= 8^6 = 12 = -1
 \end{aligned}$$

3226 This proves that tiny-jubjub is SNARK-friendly. We can write the tiny-jubjub curve in its  
3227 affine twisted Edwards representation as follows:

$$TJJ_{13} = \{(x, y) \in \mathbb{F}_{13} \times \mathbb{F}_{13} \mid 3 \cdot x^2 + y^2 = 1 + 8 \cdot x^2 \cdot y^2\} \quad (5.20)$$

3228 Now that we have the abstract definition of our tiny-jubjub curve in twisted Edwards form,  
3229 we can compute the set of points by inserting all pairs  $(x, y) \in \mathbb{F}_{13} \times \mathbb{F}_{13}$ , similarly to how we  
3230 computed the curve points in its Weierstraß or Edwards representation. We get the following:

$$\begin{aligned}
 TJJ_{13} = \{ &(0, 1), (0, 12), (1, 2), (1, 11), (2, 6), (2, 7), (3, 0), (5, 5), (5, 8), (6, 4), \\
 &(6, 9), (7, 4), (7, 9), (8, 5), (8, 8), (10, 0), (11, 6), (11, 7), (12, 2), (12, 11) \}
 \end{aligned} \quad (5.21)$$

3231

```

3232 sage: F13 = GF(13)                                     366
3233 sage: L_ETJJ = []                                       367
3234 ....: for x in F13:                                     368
3235 ....:     for y in F13:                                 369
3236 ....:         if F13(3)*x^2 + y^2 == 1+ F13(8)*x^2*y^2: 370
3237 ....:             L_ETJJ.append((x, y))                 371
3238 sage: ETJJ = Set(L_ETJJ)                               372

```

**Twisted Edwards group law** As we have seen, twisted Edwards curves are equivalent to Montgomery curves, and, as such, also have a group law. However, in contrast to Montgomery and Weierstraß curves, the group law of SNARK-friendly twisted Edwards curves can be described by a single computation that works in all cases, no matter if we add the neutral element, the inverse, or if we have to double a point. To see what the group law looks like, first observe that the point  $(0, 1)$  is a solution to  $a \cdot x^2 + y^2 = 1 + d \cdot x^2 \cdot y^2$  for any curve. The sum of any two points  $(x_1, y_1), (x_2, y_2)$  on an Edwards curve  $E(\mathbb{F})$  is then given by the following equation:

$$(x_1, y_1) \oplus (x_2, y_2) = \left( \frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right) \quad (5.22)$$

and it can be shown that the point  $(0, 1)$  serves as the neutral element and the inverse of a point  $(x_1, y_1)$  is given by  $(-x_1, y_1)$ .

*Example 83.* Lets look at the tiny-jubjub curve in Edwards form from example 5.20 again. As we have seen, this curve is given by

check  
reference

$$TJJ\_13 = \{(0, 1), (0, 12), (1, 2), (1, 11), (2, 6), (2, 7), (3, 0), (5, 5), (5, 8), (6, 4), (6, 9), (7, 4), (7, 9), (8, 5), (8, 8), (10, 0), (11, 6), (11, 7), (12, 2), (12, 11)\}$$

To get an understanding of the twisted Edwards addition law, let's first add the neutral element  $(0, 1)$  to itself. We apply the group law 5.22 and get the following:

check  
reference

$$\begin{aligned} (0, 1) \oplus (0, 1) &= \left( \frac{0 \cdot 1 + 1 \cdot 0}{1 + 8 \cdot 0 \cdot 0 \cdot 1 \cdot 1}, \frac{1 \cdot 1 - 3 \cdot 0 \cdot 0}{1 - 8 \cdot 0 \cdot 0 \cdot 1 \cdot 1} \right) \\ &= (0, 1) \end{aligned}$$

So, as expected, the neutral element added to itself gives the neutral element again. Now let's add the neutral element to some other curve point. We get the following:

$$\begin{aligned} (0, 1) \oplus (8, 5) &= \left( \frac{0 \cdot 5 + 1 \cdot 8}{1 + 8 \cdot 0 \cdot 8 \cdot 1 \cdot 5}, \frac{1 \cdot 5 - 3 \cdot 0 \cdot 8}{1 - 8 \cdot 0 \cdot 8 \cdot 1 \cdot 5} \right) \\ &= (8, 5) \end{aligned}$$

Again, as expected, adding the neutral element to any element will result in that element again. Given any curve point  $(x, y)$ , we know that its inverse is given by  $(-x, y)$ . To see how the addition of a point to its inverse works, we compute as follows:

$$\begin{aligned} (5, 5) \oplus (8, 5) &= \left( \frac{5 \cdot 5 + 5 \cdot 8}{1 + 8 \cdot 5 \cdot 8 \cdot 5 \cdot 5}, \frac{5 \cdot 5 - 3 \cdot 5 \cdot 8}{1 - 8 \cdot 5 \cdot 8 \cdot 5 \cdot 5} \right) \\ &= \left( \frac{12 + 1}{1 + 5}, \frac{12 - 3}{1 - 5} \right) \\ &= \left( \frac{0}{6}, \frac{12 + 10}{1 + 8} \right) \\ &= \left( 0, \frac{9}{9} \right) \\ &= (0, 1) \end{aligned}$$

Adding a curve point to its inverse gives the neutral element, as expected. As we have seen from these examples, the twisted Edwards addition law handles edge cases particularly well and in a unified way.

## 5.2 Elliptic Curve Pairings

As we have seen in equation 4.5, some groups come with the notation of a so-called pairing map, which is a non-degenerate bilinear map from two groups into another group.

check  
reference

In this section, we discuss **pairings on elliptic curves**, which form the basis of several zk-SNARKs and other zero-knowledge proof schemes. The SNARKs derived from pairings have the advantage of constant proof sizes, which is crucial to blockchains.

We start out by defining elliptic curve pairings and discussing a simple application which bears some resemblance to more advanced SNARKs. We then introduce the pairings arising from elliptic curves and describe Miller's algorithm, which makes these pairings practical rather than just theoretically interesting.

Elliptic curves have a few structures, like the Weil or the Tate map that qualifies as pairing.

either ex-  
pand on  
this or  
delete it

**Embedding Degrees** As we will see in what follows, every elliptic curve gives rise to a pairing map. However, we will also see in example XXX that not every such pairing can be efficiently computed. In order to distinguish curves with efficiently computable pairings from the rest, we need to start with an introduction to the so-called **embedding degree** of a curve.

add refer-  
ence

### Definition 5.2.0.1. Embedding degree

Let  $\mathbb{F}$  be a finite field, let  $E(\mathbb{F})$  be an elliptic curve over  $\mathbb{F}$ , and let  $n$  be a prime number that divides the order of  $E(\mathbb{F})$ . The embedding degree of  $E(\mathbb{F})$  with respect to  $n$  is then the smallest integer  $k$  such that  $n$  divides  $q^k - 1$ .

Fermat's little theorem (page 21 ff.) implies that every curve has at least **some** embedding degree  $k$ , since at least  $k = n - 1$  is always a solution to the congruency  $q^k \equiv 1 \pmod{n}$ . This implies that the remainder of the integer division of  $q^k - 1$  by  $n$  is 0.

check  
reference

*Example 84.* To get a better intuition of the embedding degree, let's consider the elliptic curve  $E_1(\mathbb{F}_5)$  from example 68. We know from 68 that the order of  $E_1(\mathbb{F}_5)$  is 9, and, since the only prime factor of 9 is 3, we compute the embedding degree of  $E_1(\mathbb{F}_5)$  with respect to 3.

check  
reference

To find the embedding degree, we have to find the smallest integer  $k$  such that 3 divides  $q^k - 1 = 5^k - 1$ . We try and increment until we find a proper  $k$ .

check  
reference

$k = 1: 5^1 - 1 = 4$	not divisible by 3
$k = 2: 5^2 - 1 = 24$	divisible by 3

Now we know that the embedding degree of  $E_1(\mathbb{F}_5)$  is 2 relative to the prime factor 3.

*Example 85.* Let us consider the tiny-jubjub curve  $TJJ\_13$  from example 69. We know from 69 that the order of  $TJJ\_13$  is 20, and that the order therefore has two prime factors. A "large" prime factor 5 and a small prime factor 2.

check  
reference

We start by computing the embedding degree of  $TJJ\_13$  with respect to the large prime factor 5. To find that embedding degree, we have to find the smallest integer  $k$  such that 5 divides  $q^k - 1 = 13^k - 1$ . We try and increment until we find a proper  $k$ .

check  
reference

$k = 1: 13^1 - 1 = 12$	not divisible by 5
$k = 2: 13^2 - 1 = 168$	not divisible by 5
$k = 3: 13^3 - 1 = 2196$	not divisible by 5
$k = 4: 13^4 - 1 = 28560$	divisible by 5

Now we know that the embedding degree of  $TJJ\_13$  is 4 relative to the prime factor 5.

In real-world applications, like on pairing-friendly elliptic curves such as BLS\_12-381, usually only the embedding degree of the large prime factor is relevant, which in the case of our tiny-jubjub curve is represented by 5. It should be noted, however that every prime factor of a curve's order has its own notation of embedding degree despite the fact that this is mostly irrelevant in applications.

To find the embedding degree of the small prime factor 2, we have to find the smallest integer  $k$  such that 2 divides  $q^k - 1 = 13^k - 1$ . We try and increment until we find a proper  $k$ .

$$k = 1: 13^1 - 1 = 12 \quad \text{divisible by 2}$$

Now we know that the embedding degree of  $TJJ\_13$  is 1 relative to the prime factor 2. As we have seen, different prime factors can have different embedding degrees in general.

```

sage: p = 13
sage: # large prime factor
sage: n = 5
sage: for k in range(1,5): # Fermat's little theorem
.....:     if (p^k-1)%n == 0:
.....:         break
sage: k
4
sage: # small prime factor
sage: n = 2
sage: for k in range(1,2): # Fermat's little theorem
.....:     if (p^k-1)%n == 0:
.....:         break
sage: k
1
```

*Example 86.* To give an example of a cryptographically secure real-world elliptic curve that does not have a small embedding degree, let's look at curve Secp256k1 again. We know from 70 that the order of this curve is a prime number, so we only have a single embedding degree.

To test potential embedding degrees  $k$ , say, in the range  $1 \dots 1000$ , we can invoke Sage and compute as follows:

```

sage: p = 1157920892373161954235709850086879078532699846656405
      64039457584007908834671663
sage: n = 1157920892373161954235709850086879078528375642790749
      04382605163141518161494337
sage: for k in range(1,1000):
.....:     if (p^k-1)%n == 0:
.....:         break
sage: k
999
```

We see that Secp256k1 has at least no embedding degree  $k < 1000$ , which renders Secp256k1 a curve that has no small embedding degree. This property will be of importance later on.

**Elliptic Curves over extension fields** Suppose that  $p$  is a prime number, and  $\mathbb{F}_p$  its associated prime field. We know from equation 4.36 that the fields  $\mathbb{F}_{p^m}$  are extensions of  $\mathbb{F}_p$  in the sense

check  
reference

check  
reference



3323 that  $\mathbb{F}_p$  is a subfield of  $\mathbb{F}_{p^m}$ . This implies that we can extend the affine plane that an elliptic  
 3324 curve is defined on by changing the base field to any extension field. To be more precise, let  
 3325  $E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid y^2 = x^3 + a \cdot x + b\}$  be an affine short Weierstraß curve, with parameters  
 3326  $a$  and  $b$  taken from  $\mathbb{F}$ . If  $\mathbb{F}'$  is an extension field of  $\mathbb{F}$ , then we extend the domain of the curve  
 3327 by defining  $E(\mathbb{F}')$  as follows:

$$E(\mathbb{F}') = \{(x, y) \in \mathbb{F}' \times \mathbb{F}' \mid y^2 = x^3 + a \cdot x + b\} \quad (5.23)$$

3328 While we did not change the defining parameters, we consider curve points from the affine  
 3329 plane over the extension field now. Since  $\mathbb{F} \subset \mathbb{F}'$ , it can be shown that the original elliptic curve  
 3330  $E(\mathbb{F})$  is a sub-curve of the extension curve  $E(\mathbb{F}')$ .

*Example 87.* Consider the prime field  $\mathbb{F}_5$  from example 62 and the elliptic curve  $E_1(\mathbb{F}_5)$  from  
 example 68. Since we know from XXX that  $\mathbb{F}_{5^2}$  is an extension field of  $\mathbb{F}_5$ , we can extend the  
 definition of  $E_1(\mathbb{F}_5)$  to define a curve over  $\mathbb{F}_{5^2}$ :

$$E_1(\mathbb{F}_{5^2}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid y^2 = x^3 + x + 1\}$$

3331 Since  $\mathbb{F}_{5^2}$  contains 25 points, in order to compute the set  $E_1(\mathbb{F}_{5^2})$ , we have to try  $25 \cdot 25 = 625$   
 3332 pairs, which is probably a bit too much for the average motivated reader. Instead, we invoke  
 3333 Sage to compute the curve for us. To do, we so choose the representation of  $\mathbb{F}_{5^2}$  from XXX. We  
 3334 get:

3335	<code>sage: F5= GF(5)</code>	395
3336	<code>sage: F5t.&lt;t&gt; = F5[]</code>	396
3337	<code>sage: P = F5t(t^2+2)</code>	397
3338	<code>sage: P.is_irreducible()</code>	398
3339	<code>True</code>	399
3340	<code>sage: F5_2.&lt;t&gt; = GF(5^2, name='t', modulus=P)</code>	400
3341	<code>sage: E1F5_2 = EllipticCurve(F5_2, [1, 1])</code>	401
3342	<code>sage: E1F5_2.order()</code>	402
3343	<code>27</code>	403

The curve  $E_1(\mathbb{F}_{5^2})$  consist of 27 points, in contrast to curve  $E_1(\mathbb{F}_5)$ , which consists of 9 points.  
 Printing the points gives the following:

$$\begin{aligned} E_1(\mathbb{F}_{5^2}) = \{ & \mathcal{O}, (0, 4), (0, 1), (3, 4), (3, 1), (4, 3), (4, 2), (2, 4), (2, 1), \\ & (4t + 3, 3t + 4), (4t + 3, 2t + 1), (3t + 2, t), (3t + 2, 4t), \\ & (2t + 2, t), (2t + 2, 4t), (2t + 1, 4t + 4), (2t + 1, t + 1), \\ & (2t + 3, 3), (2t + 3, 2), (t + 3, 2t + 4), (t + 3, 3t + 1), \\ & (3t + 1, t + 4), (3t + 1, 4t + 1), (3t + 3, 3), (3t + 3, 2), (1, 4t) \} \end{aligned}$$

3344 As we can see, curve  $E_1(\mathbb{F}_5)$  sits inside curve  $E(\mathbb{F}_{5^2})$ , which is implied by  $\mathbb{F}_5$  being a subfield  
 3345 of  $\mathbb{F}_{5^2}$ .

3346 **Full torsion groups** The fundamental theorem of finite cyclic groups XXX implies that every  
 3347 prime factor  $n$  of a cyclic group's order defines a subgroup of the size of the prime factor. Such  
 3348 a subgroup is called an  $n$ -torsion group. We have seen many of those subgroups in the examples  
 3349 XXX and XXX.

3350 When we consider elliptic curve extensions as defined in 5.23, we could ask what happens  
 3351 to the  $n$ -torsion groups in the extension. One might intuitively think that their extension just



parallels the extension of the curve. For example, when  $E(\mathbb{F}_p)$  is a curve over prime field  $\mathbb{F}_p$ , with some  $n$ -torsion group  $\mathbb{G}$  and when we extend the curve to  $E(\mathbb{F}_{p^m})$ , then there is a bigger  $n$ -torsion group such that  $\mathbb{G}$  is a subgroup. This might make intuitive sense, as  $E(\mathbb{F}_p)$  is a sub-curve of  $E(\mathbb{F}_{p^m})$ .

However, the actual situation is a bit more surprising than that. To see that, let  $\mathbb{F}_p$  be a prime field and let  $E(\mathbb{F}_p)$  be an elliptic curve of order  $r$ , with embedding degree  $k$  and  $n$ -torsion group  $E(\mathbb{F}_p)[n]$  for the same prime factor  $n$  of  $r$ . Then it can be shown that the  $n$ -torsion group  $E(\mathbb{F}_{p^m})[n]$  of a curve extension is equal to  $E(\mathbb{F}_p)[n]$ , as long as the power  $m$  is less than the embedding degree  $k$  of  $E(\mathbb{F}_p)$ .

However, for the prime power  $p^m$ , for any  $m \geq k$ ,  $E(\mathbb{F}_{p^m})[n]$  is strictly larger than  $E(\mathbb{F}_p)[n]$  and contains  $E(\mathbb{F}_p)[n]$  as a subgroup. We call the  $n$ -torsion group  $E(\mathbb{F}_{p^k})[n]$  of the extension of  $E$  over  $\mathbb{F}_{p^k}$  the **full  $n$ -torsion group** of that elliptic curve. It can be shown that it contains  $n^2$  many elements and consists of  $n + 1$  subgroups, one of which is  $E(\mathbb{F}_p)[n]$ .

So, roughly speaking, when we consider **towers of curve extensions**  $E(\mathbb{F}_{p^m})$  ordered by the prime power  $m$ , then the  $n$ -torsion group stays constant for every level  $m$ , that is smaller than the embedding degree, while it suddenly blossoms into a larger group on level  $k$  with  $n + 1$  subgroups, and then stays like that for any level  $m$  larger than  $k$ . In other words, once the extension field is big enough to find one more point of order  $n$  (that is not defined over the base field), then we actually find all of the points in the full torsion group.

*Example 88.* Consider curve  $E_1(\mathbb{F}_5)$  again. We know that it contains a 3-torsion group and that the embedding degree of 3 is 2. From this we can deduce that we can find the full 3-torsion group  $E_1[3]$  in the curve extension  $E_1(\mathbb{F}_{5^2})$ , the latter of which we computed in example 87.

Since that curve is small, in order to find the full 3-torsion, we can loop through all elements of  $E_1(\mathbb{F}_{5^2})$  and check the defining equation  $[3]P = \mathcal{O}$ . Invoking Sage, we compute as follows:

```
sage: INF = E1F5_2(0) # Point at infinity          404
sage: L_E1_3 = []                                     405
sage: for p in E1F5_2:                               406
.....:     if 3*p == INF:                             407
.....:         L_E1_3.append(p)                         408
sage: E1_3 = Set(L_E1_3) # Full 3-torsion set        409
```

We get the following result:

$$E_1[3] = \{\mathcal{O}, (1, t), (1, 4t), (2, 1), (2, 4), (2t + 1, t + 1), (2t + 1, 4t + 4), (3t + 1, t + 4), (3t + 1, 4t + 1)\}$$

*Example 89.* Consider the tiny-jubjub curve from example 69. We know from example 85 that it contains a 5-torsion group and that the embedding degree of 5 is 4. This implies that we can find the full 5-torsion group  $TJJ\_13[5]$  in the curve extension  $TJJ\_13(\mathbb{F}_{13^4})$ .

To compute the full torsion, first observe that, since  $\mathbb{F}_{13^4}$  contains 28561 elements, computing  $TJJ\_13(\mathbb{F}_{13^4})$  means checking  $28561^2 = 815730721$  elements. From each of these curve points  $P$ , we then have to check the equation  $[5]P = \mathcal{O}$ . Doing this for 815730721 is a bit too slow even on a computer.

Fortunately, Sage has a way to loop through points of a given order efficiently. The following Sage code provides a way to compute the full torsion group:

```
sage: # define the extension field                    410
sage: F13= GF(13) # prime field                      411
sage: F13t.<t> = F13[] # polynomials over t          412
```

towers  
of curve  
extensions

check  
reference

check  
reference

check  
reference

```

3395 sage: P = F13t(t^4+2) # irreducible polynomial of degree 4 413
3396 sage: P.is_irreducible() 414
3397 True 415
3398 sage: F13_4.<t> = GF(13^4, name='t', modulus=P) # F_{13^4} 416
3399 sage: TJJF13_4 = EllipticCurve(F13_4,[8,8]) # tiny-jubjub 417
3400 extension
3401 sage: # compute the full 5-torsion 418
3402 sage: L_TJJF13_4_5 = [] 419
3403 sage: INF = TJJF13_4(0) 420
3404 sage: for P in INF.division_points(5): # [5]P == INF 421
3405 ....:     L_TJJF13_4_5.append(P) 422
3406 sage: len(L_TJJF13_4_5) 423
3407 25 424
3408 sage: TJJF13_4_5 = Set(L_TJJF13_4_5) 425

```

As expected, we get a group that contains  $5^2 = 25$  elements. As it's rather tedious to write this group down, and as we don't need it in what follows, we forgo doing this. To see that the embedding degree 4 is actually the smallest prime power to find the full 5-torsion group, let's compute the 5-torsion group over of the tiny-jubjub curve of the extension field  $\mathbb{F}_{13^3}$ . We get the following:

```

3414 sage: # define the extension field 426
3415 sage: P = F13t(t^3+2) # irreducible polynomial of degree 3 427
3416 sage: P.is_irreducible() 428
3417 True 429
3418 sage: F13_3.<t> = GF(13^3, name='t', modulus=P) # F_{13^3} 430
3419 sage: TJJF13_3 = EllipticCurve(F13_3,[8,8]) # tiny-jubjub 431
3420 extension
3421 sage: # compute the 5-torsion 432
3422 sage: L_TJJF13_3_5 = [] 433
3423 sage: INF = TJJF13_3(0) 434
3424 sage: for P in INF.division_points(5): # [5]P == INF 435
3425 ....:     L_TJJF13_3_5.append(P) 436
3426 sage: len(L_TJJF13_3_5) 437
3427 5 438
3428 sage: TJJF13_3_5 = Set(L_TJJF13_3_5) # full 5-torsion 439

```

As we can see, the 5-torsion group of tiny-jubjub over  $\mathbb{F}_{13^3}$  is equal to the 5-torsion group of tiny-jubjub over  $\mathbb{F}_{13}$  itself.

*Example 90.* Let's look at the curve Secp256k1. We know from example 70 that the curve is of some prime order  $r$ . Because of this, the only  $n$ -torsion group to consider is the curve itself, so the curve group is the  $r$ -torsion.

check  
reference

However, in order to find the full  $r$ -torsion of Secp256k1, we need to compute the embedding degree  $k$ . And as we have seen in XXX it is at least not small. However, we know from Fermat's little theorem (page 21 ff.) that a finite embedding degree must exist. It can be shown that it is given by the following 256-bit number:

add refer-  
ence

$$k = 192986815395526992372618308347813175472927379845817397100860523586360249056$$

This means that the embedding degree is **very large**, which implies that the field extension  $\mathbb{F}_{p^k}$  is very large too. To understand how big  $\mathbb{F}_{p^k}$  is, recall that an element of  $\mathbb{F}_{p^m}$  can be represented as

a string  $[x_0, \dots, x_m]$  of  $m$  elements, each containing a number from the prime field  $\mathbb{F}_p$ . Now, in the case of Secp256k1, such a representation has  $k$ -many entries, each of them 256 bits in size. So, without any optimizations, representing such an element would need  $k \cdot 256$  bits, which is too much to be represented in the observable universe.

**Torsion subgroups** As we have stated above, any full  $n$ -torsion group contains  $n + 1$  cyclic subgroups, two of which are of particular interest in pairing-based elliptic curve cryptography. To characterize these groups, we need to consider the so-called **Frobenius endomorphism** of an elliptic curve  $E(\mathbb{F})$  over some finite field  $\mathbb{F}$  of characteristic  $p$ :

$$\pi : E(\mathbb{F}) \rightarrow E(\mathbb{F}) : \begin{array}{ccc} (x, y) & \mapsto & (x^p, y^p) \\ \mathcal{O} & \mapsto & \mathcal{O} \end{array} \quad (5.24)$$

It can be shown that  $\pi$  maps curve points to curve points. The first thing to note is that, in case  $\mathbb{F}$  is a prime field, the Frobenius endomorphism acts trivially, since  $(x^p, y^p) = (x, y)$  on prime fields due to Fermat's little theorem (page 21 ff.). This means that the Frobenius map is more interesting over prime field extensions.

check  
reference

With the Frobenius map at hand, we can characterize two important subgroups of the full  $n$ -torsion. The first subgroup is the  $n$ -torsion group that already exists in the curve over the base field. In pairing-based cryptography, this group is usually written as  $\mathbb{G}_1$ , assuming that the prime factor  $n$  in the definition is implicitly given. Since we know that the Frobenius map acts trivially on curves over the prime field, we can define  $\mathbb{G}_1$  as follows:

$$\mathbb{G}_1[n] := \{(x, y) \in E[n] \mid \pi(x, y) = (x, y)\} \quad (5.25)$$

In more mathematical terms, this definition means that  $\mathbb{G}_1$  is the **Eigenspace** of the Frobenius map with respect to the **Eigenvalue 1**.

It can be shown that there is another subgroup of the full  $n$ -torsion group that can be characterized by the Frobenius map. In the context of so-called **type 3 pairing-based cryptography**, this subgroup is usually called  $\mathbb{G}_2$  and it is defined as follows:

$$\mathbb{G}_2[n] := \{(x, y) \in E[n] \mid \pi(x, y) = [p](x, y)\} \quad (5.26)$$

S: either  
add more  
explanation  
or  
move to a  
footnote

In mathematical terms,  $\mathbb{G}_2$  is the **Eigenspace** of the Frobenius map with respect to the **Eigenvalue  $p$** .

type 3  
pairing-  
based  
cryptogra-  
phy

*Notation and Symbols 11.* If the prime factor  $n$  of a curve's order is clear from the context, we sometimes simply write  $\mathbb{G}_1$  and  $\mathbb{G}_2$  to mean  $\mathbb{G}_1[n]$  and  $\mathbb{G}_2[n]$ , respectively.

It should be noted, however that other definitions of  $\mathbb{G}_2$  also exists in the literature. However, in the context of pairing-based cryptography, this is the most common one. It is particularly useful because we can define hash functions that map into  $\mathbb{G}_2$ , which is not possible for all subgroups of the full  $n$ -torsion.

add refer-  
ences?

*Example 91.* Consider the curve  $E_1(\mathbb{F}_5)$  from example 68 again. As we have seen, this curve has the embedding degree  $k = 2$ , and a full 3-torsion group is given as follows:

$$E_1[3] = \{\mathcal{O}, (2, 1), (2, 4), (1, t), (1, 4t), (2t + 1, t + 1), (2t + 1, 4t + 4), (3t + 1, t + 4), (3t + 1, 4t + 1)\} \quad (5.27)$$

According to the general theory,  $E_1[3]$  contains 4 subgroups, and we can characterize the subgroups  $\mathbb{G}_1$  and  $\mathbb{G}_2$  using the Frobenius endomorphism. Unfortunately, at the time of writing,

Sage does not have a predefined Frobenius endomorphism for elliptic curves, so we have to use the Frobenius endomorphism of the underlying field as a temporary workaround. We compute as follows:

```

3473 sage: L_G1 = []
3474 sage: for P in E1_3:
3475     ....:     PiP = E1F5_2([a.frobenius() for a in P]) # pi(P)
3476     ....:     if P == PiP:
3477     ....:         L_G1.append(P)
3478 sage: G1 = Set(L_G1)

```

As expected, the group  $\mathbb{G}_1 = \{\mathcal{O}, (2, 4), (2, 1)\}$  is identical to the 3-torsion group of the (unextended) curve over the prime field  $E_1(\mathbb{F}_5)$ . We can use almost the same algorithm to compute the group  $\mathbb{G}_2$  and get the following:

```

3482 sage: L_G2 = []
3483 sage: for P in E1_3:
3484     ....:     PiP = E1F5_2([a.frobenius() for a in P]) # pi(P)
3485     ....:     pP = 5*P # [5]P
3486     ....:     if pP == PiP:
3487     ....:         L_G2.append(P)
3488 sage: G2 = Set(L_G2)

```

Thus, we have computed the the second subgroup of the full 3-torsion group of curve  $E_1$  as the set  $\mathbb{G}_2 = \{\mathcal{O}, (1, t), (1, 4t)\}$ .

*Example 92.* Consider the tiny-jubjub curve *TJJ\_13* from example 69. In example 89, we computed its full 5 torsion, which is a group that has 6 subgroups. We compute  $G_1$  using Sage as follows:

```

3494 sage: L_TJJ_G1 = []
3495 sage: for P in TJJF13_4_5:
3496     ....:     PiP = TJJF13_4([a.frobenius() for a in P]) # pi(P)
3497     ....:     if P == PiP:
3498     ....:         L_TJJ_G1.append(P)
3499 sage: TJJ_G1 = Set(L_TJJ_G1)

```

We get  $\mathbb{G}_1 = \{\mathcal{O}, (7, 2), (8, 8), (8, 5), (7, 11)\}$

```

3501 sage: L_TJJ_G1 = []
3502 sage: for P in TJJF13_4_5:
3503     ....:     PiP = TJJF13_4([a.frobenius() for a in P]) # pi(P)
3504     ....:     pP = 13*P # [5]P
3505     ....:     if pP == PiP:
3506     ....:         L_TJJ_G1.append(P)
3507 sage: TJJ_G1 = Set(L_TJJ_G1)

```

$\mathbb{G}_2 = \{\mathcal{O}, (9t^2 + 7, t^3 + 11t), (9t^2 + 7, 12t^3 + 2t), (4t^2 + 7, 5t^3 + 10t), (4t^2 + 7, 8t^3 + 3t)\}$

*Example 93.* Consider Bitcoin's curve Secp256k1 again. Since the group  $\mathbb{G}_1$  is identical to the torsion group of the unextended curve, and since Secp256k1 has prime order, we know that, in this case,  $\mathbb{G}_1$  is identical to Secp256k1. It is however, infeasible not to compute not only  $\mathbb{G}_2$  itself, but to even compute an average element of  $\mathbb{G}_2$ , as elements need too much storage to be

check  
reference

check  
reference

3513 representable in this universe.

3514 **The Weil pairing** In this part, we consider a pairing function defined on the subgroups  $\mathbb{G}_1[r]$   
 3515 and  $\mathbb{G}_2[r]$  of the full  $r$ -torsion  $E[r]$  of a short Weierstraß elliptic curve. To be more precise, let  
 3516  $E(\mathbb{F}_p)$  be an elliptic curve of embedding degree  $k$  such that  $r$  is a prime factor of its order. Then  
 3517 the **Weil pairing** is a bilinear, non-degenerate map:

$$e(\cdot, \cdot) : \mathbb{G}_1[r] \times \mathbb{G}_2[r] \rightarrow \mathbb{F}_{p^k} ; (P, Q) \mapsto (-1)^r \cdot \frac{f_{r,P}(Q)}{f_{r,Q}(P)} \quad (5.28)$$

The extension field elements  $f_{r,P}(Q), f_{r,Q}(P) \in \mathbb{F}_{p^k}$  are computed by **Miller's algorithm**:

check  
floating of  
algorithm

---

**Algorithm 7** Miller's algorithm for short Weierstraß curves  $y^2 = x^3 + ax + b$

---

**Require:**  $r > 3, P \in E[r], Q \in E[r]$  and

$b_0, \dots, b_t \in \{0, 1\}$  with  $r = b_0 \cdot 2^0 + b_1 \cdot 2^1 + \dots + b_t \cdot 2^t$  and  $b_t = 1$

**procedure** MILLER'S ALGORITHM( $P, Q$ )

**if**  $P = \mathcal{O}$  or  $Q = \mathcal{O}$  or  $P = Q$  **then**

**return**  $f_{r,P}(Q) \leftarrow (-1)^r$

**end if**

$(x_T, y_T) \leftarrow (x_P, y_P)$

$f_1 \leftarrow 1$

$f_2 \leftarrow 1$

**for**  $j \leftarrow t - 1, \dots, 0$  **do**

$m \leftarrow \frac{3 \cdot x_T^2 + a}{2 \cdot y_T}$

$f_1 \leftarrow f_1^2 \cdot (y_Q - y_T - m \cdot (x_Q - x_T))$

$f_2 \leftarrow f_2^2 \cdot (x_Q + 2x_T - m^2)$

$x_{2T} \leftarrow m^2 - 2x_T$

$y_{2T} \leftarrow -y_T - m \cdot (x_{2T} - x_T)$

$(x_T, y_T) \leftarrow (x_{2T}, y_{2T})$

**if**  $b_j = 1$  **then**

$m \leftarrow \frac{y_T - y_P}{x_T - x_P}$

$f_1 \leftarrow f_1 \cdot (y_Q - y_T - m \cdot (x_Q - x_T))$

$f_2 \leftarrow f_2 \cdot (x_Q + (x_P + x_T) - m^2)$

$x_{T+P} \leftarrow m^2 - x_T - x_P$

$y_{T+P} \leftarrow -y_T - m \cdot (x_{T+P} - x_T)$

$(x_T, y_T) \leftarrow (x_{T+P}, y_{T+P})$

**end if**

**end for**

$f_1 \leftarrow f_1 \cdot (x_Q - x_T)$

**return**  $f_{r,P}(Q) \leftarrow \frac{f_1}{f_2}$

**end procedure**

---

3518 Understanding how the algorithm works in detail requires the concept of **divisors**, which is  
 3519 outside of the scope this book. The interested reader might look at XXX.

3520 In real-world applications of pairing-friendly elliptic curves, the embedding degree is usu-  
 3521 ally a small number like 2, 4, 6 or 12, and the number  $r$  is the largest prime factor of the curve's  
 3522 order.  
 3523

add refer-  
ences

3524 *Example 94.* Consider curve  $E_1(\mathbb{F}_5)$  from example 68. Since the only prime factor of the  
 3525 group's order is 3, we cannot compute the Weil pairing on this group using our definition of  
 3526 Miller's algorithm. In fact, since  $\mathbb{G}_1$  is of order 3, executing the if statement on line XXX will  
 3527 lead to a "division by zero" error in the computation of the slope  $m$ .

check  
reference  
add refer-  
ence

*Example 95.* Consider the tiny-jubjub curve  $TJJ\_13(\mathbb{F}_{13})$  from example 69 again. We want to  
 instantiate the general definition of the Weil pairing for this example. To do so, recall that, as we  
 have see in example 85, its embedding degree is 4, and that we have the following type-3 pairing  
 groups (where  $\mathbb{G}_1$  and  $\mathbb{G}_2$  are subgroups of the full 5-torsion found in the curve  $TJJ\_13(\mathbb{F}_{13^4})$ ):

check  
reference  
check  
reference

$$\mathbb{G}_1 = \{\mathcal{O}, (7, 2), (8, 8), (8, 5), (7, 11)\}$$

$$\mathbb{G}_2 = \{\mathcal{O}, (9t^2 + 7, t^3 + 11t), (9t^2 + 7, 12t^3 + 2t), (4t^2 + 7, 5t^3 + 10t), (4t^2 + 7, 8t^3 + 3t)\}$$

3528 The type-3 Weil pairing is a map  $e(\cdot, \cdot) : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{F}_{13^4}$ . From the first if-statement in  
 3529 Miller's algorithm, we can deduce that  $e(\mathcal{O}, Q) = 1$  as well as  $e(P, \mathcal{O}) = 1$  for all arguments  
 3530  $P \in \mathbb{G}_1$  and  $Q \in \mathbb{G}_2$ . In order to compute a non-trivial Weil pairing, we choose the arguments  
 3531  $P = (7, 2)$  and  $Q = (9t^2 + 7, 12t^3 + 2t)$ .

3532 To compute the pairing  $e((7, 2), (9t^2 + 7, 12t^3 + 2t))$ , we have to compute the extension field  
 3533 elements  $f_{5,P}(Q)$  and  $f_{5,Q}(P)$  by applying Miller's algorithm. Do do so, observe that we have  
 3534  $5 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2$ , so we get  $t = 2$  as well as  $b_0 = 1, b_1 = 0$  and  $b_2 = 1$ . The loop therefore  
 3535 needs to be executed two times.

Computing  $f_{5,P}(Q)$ , we initiate  $(x_T, y_T) = (7, 2)$  as well as  $f_1 = 1$  and  $f_2 = 1$ . Then we  
 proceed as follows:

$j$	$b_j$	$m$	$f_1$	$f_2$	$x_{2T}$	$y_{2T}$	$x_{T+P}$	$y_{T+P}$
1	.							

$$\begin{aligned}
m &= \frac{3 \cdot x_T^2 + a}{2 \cdot y_T} \\
&= \frac{3 \cdot 2^2 + 1}{2 \cdot 4} = \frac{3}{3} \\
&= 1
\end{aligned}$$

$$\begin{aligned}
f_1 &= f_1^2 \cdot (y_Q - y_T - m \cdot (x_Q - x_T)) \\
&= 1^2 \cdot (t - 4 - 1 \cdot (1 - 2)) = t - 4 + 1 \\
&= t + 2
\end{aligned}$$

$$\begin{aligned}
f_2 &= f_2^2 \cdot (x_Q + 2x_T - m^2) \\
&= 1^2 \cdot (1 + 2 \cdot 2 - 1^2) = (1 + 4 - 1) \\
&= 4
\end{aligned}$$

$$\begin{aligned}
x_{2T} &= m^2 - 2x_T \\
&= 1^2 - 2 \cdot 2 = -3 \\
&= 2
\end{aligned}$$

$$\begin{aligned}
y_{2T} &= -y_T - m \cdot (x_{2T} - x_T) \\
&= -4 - 1 \cdot (2 - 2) = -4 \\
&= 1
\end{aligned}$$

We update  $(x_T, y_T) = (2, 1)$  and, since  $b_0 = 1$ , we have to execute the if statement on line XXX in the **for** loop. However, since we only loop a single time, we don't need to compute  $y_{T+P}$ , since we only need the updated  $x_T$  in the final step. We get:

$$\begin{aligned}
m &= \frac{y_T - y_P}{x_T - x_P} \\
&= \frac{1 - 4}{2 - x_P}
\end{aligned}$$

$$f_1 = f_1 \cdot (y_Q - y_T - m \cdot (x_Q - x_T))$$

$$f_2 = f_2 \cdot (x_Q + (x_P + x_T) - m^2)$$

$$x_{T+P} = m^2 - x_T - x_P$$

add reference

should all lines of all algorithms be numbered?

## 3536 5.3 Hashing to Curves

3537 Elliptic curve cryptography frequently requires the ability to hash data onto elliptic curves. If  
3538 the order of the curve is not a prime number, hashing to prime number subgroups is also of



importance. In the context of pairing-friendly curves, it is also sometimes necessary to hash specifically onto the group  $\mathbb{G}_1$  or  $\mathbb{G}_2$ .

As we have seen in section 4.1.2, many general methods are known for hashing into groups in general, and finite cyclic groups in particular. As elliptic groups are cyclic, those methods can be utilized in this case, too. However, in what follows we want to describe some methods specific to elliptic curves that are frequently used in real-world applications.

check  
reference

**Try-and-increment hash functions** One of the most straight-forward ways of hashing a bit-string onto an elliptic curve point in a secure way is to use a cryptographic hash function together with one of the methods we described in section 4.1.2 to hash to the modular arithmetic base field of the curve. Ideally, the hash function generates an image that is at least one bit longer than the bit representation of the base field modulus.

check  
reference

The image in the base field can then be interpreted as the  $x$  coordinate of the curve point, and the two possible  $y$  coordinates are derived from the curve equation, while one of the bits that exceeded the modulus determines which of the two  $y$  coordinates to choose.

Such an approach would be deterministic and easy to implement, and it would conserve the cryptographic properties of the original hash function. However, not all  $x$  coordinates generated in such a way will result in quadratic residues when inserted into the defining equation. It follows that not all field elements give rise to actual curve points. In fact, on a prime field, only half of the field elements are quadratic residues. Hence, assuming an even distribution of the hash values in the field, this method would fail to generate a curve point in about half of the attempts.

One way to account for this problem is the so-called **try-and-increment** method. Its basic assumption is that, when hashing different values, the result will eventually lead to a valid curve point.

Therefore, instead of simply hashing a string  $s$  to the field, we hash the concatenation of  $s$  with additional bytes to the field instead. In other words, we use a try-and-increment hash as described in 5. If the first try of hashing to the field does not result in a valid curve point, the counter is incremented, and the hashing is repeated again. This is done until a valid curve point is found.

check  
reference

This method has a number of advantages: It is relatively easy to implement in code, and it maintains the cryptographic properties of the original hash function. However, it is not guaranteed to find a valid curve point, as there is a chance that all possible values in the chosen size of the counter will fail to generate a quadratic residue. Fortunately, it is possible to make the probability for this arbitrarily small by choosing large enough counters and relying on the (approximate) uniformity of the hash-to-field function.

check if  
the algo-  
rithm is  
floated  
properly

If the curve is not of prime order, the result will be a general curve point that might not be in the “large” prime-order subgroup. In this case, a **cofactor clearing** step is then necessary to project the curve point onto the subgroup. This is done by scalar multiplication with the cofactor of prime order with respect to the curves order.

*Example 96.* Consider the tiny-jubjub curve from example 69. We want to construct a try-and-increment hash function that hashes a binary string  $s$  of arbitrary length onto the large prime-order subgroup of size 5.

check  
reference

Since the curve, as well as our targeted subgroup, is defined over the field  $\mathbb{F}_{13}$ , and the binary representation of 13 is  $13.bits() = 1101$ , we apply SHA256 from Sage’s hashlib library on the concatenation  $s||c$  for some binary counter string, and use the first 4 bits of the image to try to hash into  $\mathbb{F}_{13}$ . In case we are able to hash to a value  $z$  such that  $z^3 + 8 \cdot z + 8$  is a quadratic residue in  $\mathbb{F}_{13}$ , we use the 5-th bit to decide which of the two possible roots of  $z^3 + 8 \cdot z + 8$  we



**Algorithm 8** Hash-to- $E(\mathbb{F}_r)$ **Require:**  $r \in \mathbb{Z}$  with  $r.\text{nbits}() = k$  and  $s \in \{0, 1\}^*$ **Require:** Curve equation  $y^2 = x^3 + ax + b$  over  $\mathbb{F}_r$ **procedure** TRY-AND-INCREMENT( $r, k, s$ ) $c \leftarrow 0$ **repeat** $s' \leftarrow s || c.\text{bits}()$  $z \leftarrow H(s')_0 \cdot 2^0 + H(s')_1 \cdot 2^1 + \dots + H(s')_k \cdot 2^k$  $x \leftarrow z^3 + a \cdot z + b$  $c \leftarrow c + 1$ **until**  $z < r$  and  $x^{\frac{r-1}{2}} \bmod r = 1$ **if**  $H(s')_{k+1} == 0$  **then** $y \leftarrow \sqrt{x} \#(\text{root in } \mathbb{F}_r)$ **else** $y \leftarrow r - \sqrt{x} \#(\text{root in } \mathbb{F}_r)$ **end if****return**  $(x, y)$ **end procedure****Ensure:**  $(x, y) \in E(\mathbb{F}_r)$ 

will choose as the  $y$  coordinate. The result is a curve point different from the point at infinity. To project it to a point of  $\mathbb{G}_1$ , we multiply it with the cofactor 4. If the result is still not the point at infinity, it is the result of the hash.

To make this concrete, let  $s = '10011001111010110100000111'$  be our binary string that we want to hash onto  $\mathbb{G}_1$ . We use a 4-bit binary counter starting at zero, that is, we choose  $c = 0000$ . Invoking Sage, we define the try-hash function as follows:

```

sage: import hashlib
sage: def try_hash(s, c):
.....:     s_1 = s+c
.....:     hasher = hashlib.sha256(s_1.encode('utf-8'))
.....:     digest = hasher.hexdigest()
.....:     d = Integer(digest, base=16)
.....:     sign = d.str(2)[-5:-4]
.....:     d = d.str(2)[-4:]
.....:     z = Integer(d, base=2)
.....:     return (z, sign)
sage: try_hash('10011001111010110100000111', '0000')
(15, '1')
```

As we can see, our first attempt to hash into  $\mathbb{F}_{13}$  was not successful, as 15 is not a number in  $\mathbb{F}_{13}$ , so we increment the binary counter by 1 and try again:

```

sage: try_hash('10011001111010110100000111', '0001')
(3, '0')
```

With this try, we found a hash into  $\mathbb{F}_{13}$ . However, this point is not guaranteed to define a curve point. To see that, we insert  $z = 3$  into the right side of the Weierstraß equation of the tiny-jubjub curve, and compute  $3^3 + 8 * 3 + 8 = 7$ . However, 7 is not a quadratic residue in

3611  $\mathbb{F}_{13}$ , since  $7^{\frac{13-1}{2}} = 7^6 = 12 = -1$ . This means that 3 is not a suitable point, and we have to  
 3612 increment the counter two more times:

```

3613 sage: try_hash('10011001111010110100000111', '0010')      480
3614 (3, '0')                                                    481
3615 sage: try_hash('10011001111010110100000111', '0011')      482
3616 (6, '1')                                                    483

```

Since  $6^3 + 8 \cdot 6 + 8 = 12$ , and we have  $\sqrt{12} \in \{5, 8\}$ , we finally found the valid  $x$  coordinate  $x = 6$  for the curve point hash. Now, since the sign bit of this hash is 1, we choose the larger root  $y = 8$  as the  $y$  coordinate and get the following hash which is a valid curve point point on the tiny-jubjub curve:

$$H('10011001111010110100000111') = (6, 8)$$

In order to project this onto the “large” prime-order subgroup, we have to do cofactor clearing, that is, we have to multiply the point with the cofactor 4. We get the following:

$$[4](6, 8) = \mathcal{O}$$

3617 This means that the hash value is still not right. We therefore have to increment the counter  
 3618 two more times again, until we finally find a correct hash to  $\mathbb{G}_1$ :

```

3619 sage: try_hash('10011001111010110100000111', '0100')      484
3620 (0, '1')                                                    485
3621 sage: try_hash('10011001111010110100000111', '0101')      486
3622 (12, '0')                                                  487

```

Since  $12^3 + 8 \cdot 12 + 8 = 12$ , and we have  $\sqrt{12} \in \{5, 8\}$ , we found another valid  $x$  coordinate  $x = 12$  for the curve point hash. Since the sign bit of this hash is 0, we choose the smaller root  $y = 5$  as the  $y$  coordinate, and get the following hash, which is a valid curve point point on the tiny-jubjub curve:

$$H('10011001111010110100000111') = (12, 5)$$

In order to project this onto the “large” prime-order subgroup we have to do cofactor clearing, again? that is, we have to multiply the point with the cofactor 4. We get the following:

$$[4](12, 5) = (8, 5)$$

3623 So, hashing the binary string '10011001111010110100000111' onto  $\mathbb{G}_1$  gives the hash value  
 3624 (8, 5) as a result.

## 3625 5.4 Constructing elliptic curves

3626 Cryptographically secure elliptic curves like Secp256k1 from example 70 have been known for  
 3627 quite some time. Given the latest advancements of cryptography, however, it is often necessary  
 3628 to design and instantiate elliptic curves from scratch that satisfy certain very specific properties.

3629 For example, in the context of SNARK development, it was necessary to design a curve that  
 3630 can be efficiently implemented inside of a so-called **circuit** in order to enable primitives like  
 3631 elliptic curve **signature schemes** in a zero-knowledge proof. Such a curve is given by the Baby-  
 3632 jubjub curve in XXX, and we have paralleled its definition by introducing the tiny-jubjub curve

check  
reference

circuit

signature  
schemes

add refer-  
ence

from example 69. As we have seen, those curves are instances of so-called twisted Edwards curves, and as such have easy to implement addition laws that work without branching. However, we introduced the tiny-jubjub curve out of thin air, as we just gave the curve parameters without explaining how we came up with them.

Another requirement in the context of many so-called **pairing-based zero-knowledge proofing systems** is the existence of a suitable, pairing-friendly curve with a specified security level and a low embedding degree as defined in 5.2.0.1. Famous examples are the BLS\_12 and the NMT curves.

The major goal of this section is to explain the most important method of designing elliptic curves with predefined properties from scratch, called the **complex multiplication method**. We will apply this method in section XXX to synthesize a particular BLS\_6 curve, which is one of the most insecure curves, but it will serve as the main curve to build our pen-and-paper SNARKs on. As we will see, this curve has a “large” prime factor subgroup of order 13, which implies that we can use our tiny-jubjub curve to implement certain elliptic curve cryptographic primitives in circuits over that BLS\_6 curve.

Before we introduce the complex multiplication method, we have to explain a few properties of elliptic curves that are of key importance in understanding the complex multiplication method.

**The Trace of Frobenius** To understand the complex multiplication method of elliptic curves, we have to define the so-called **trace** of an elliptic curve first.

We know from XXX that elliptic curves over finite fields are products of cyclic groups of finite order. Therefore, an interesting question is whether it is possible to estimate the number of elements that this curve contains. Since an affine short Weierstraß curve consists of pairs  $(x, y)$  of elements from a finite field  $\mathbb{F}_q$  plus the point at infinity, and the field  $\mathbb{F}_q$  contains  $q$  elements, the number of curve points cannot be arbitrarily large, since it can contain at most  $q^2 + 1$  many elements.

There is however, a more precise estimation, usually called the **Hasse bound**. To understand it, let  $E(\mathbb{F}_q)$  be an affine short Weierstraß curve over a finite field  $\mathbb{F}_q$  of order  $q$ , and let  $|E(\mathbb{F}_q)|$  be the order of the curve. Then there is an integer  $t \in \mathbb{Z}$ , called the **trace of Frobenius** of the curve, such that  $|t| \leq 2\sqrt{q}$  and the following equation holds:

$$|E(\mathbb{F}_q)| = q + 1 - t \quad (5.29)$$

A positive trace, therefore, implies that the curve contains less points than the underlying field, whereas a negative trace means that the curve contains more points. However, the estimation  $|t| \leq 2\sqrt{q}$  implies that the difference is not very large in either direction, and the number of elements in an elliptic curve is always approximately in the same order of magnitude as the size of the curve’s base field.

*Example 97.* Consider the elliptic curve  $E_1(\mathbb{F}_5)$  from example 68. We know that it contains 9 curve points. Since the order of  $\mathbb{F}_5$  is 5, we compute the trace of  $E_1(\mathbb{F})$  to be  $t = -3$ , since the Hasse bound is given by the following equation:

$$9 = 5 + 1 - (-3)$$

Indeed, we have  $|t| \leq 2\sqrt{q}$ , since  $\sqrt{5} > 2.23$  and  $|-3| = 3 \leq 4.46 = 2 \cdot 2.23 < 2 \cdot \sqrt{5}$ .

*Example 98.* To compute the trace of the tiny-jubjub curve, recall from example 77 that the order of  $TJJ_{13}$  is 20. Since the order of  $\mathbb{F}_{13}$  is 13, we can therefore use the Hasse bound and compute the trace as  $t = -6$ :

$$20 = 13 + 1 - (-6) \quad (5.30)$$

check  
referencecheck  
referenceadd refer-  
encesadd refer-  
encereference  
text to be  
written in  
Algebracheck  
referencecheck  
reference

3672 Again, we have  $|t| \leq 2\sqrt{q}$ , since  $\sqrt{13} > 3.60$  and  $|-6| = 6 \leq 7.20 = 2 \cdot 3.60 < 2 \cdot \sqrt{13}$ .

*Example 99.* To compute the trace of Secp256k1, recall from example 70 [that this curve is](#) defined over a prime field with  $p$  elements, and that the order of that group is given by  $r$ :

check  
reference

```
p = 115792089237316195423570985008687907853269984665640564039457584007908834671663
r = 115792089237316195423570985008687907852837564279074904382605163141518161494337
```

Using the Hesse bound  $r = p + 1 - t$ , we therefore compute  $t = p + 1 - r$ , which gives the trace of curve Secp256k1 as follows:

```
t = 432420386565659656852420866390673177327
```

3673 As we can see, Secp256k1 contains less elements than its underlying field. However, the  
3674 difference is tiny, since the order of Secp256k1 is in the same order of magnitude as the order  
3675 of the underlying field. Compared to  $p$  and  $r$ ,  $t$  is tiny.

```
3676 sage: p = 1157920892373161954235709850086879078532699846656405 488
3677         64039457584007908834671663
3678 sage: r = 1157920892373161954235709850086879078528375642790749 489
3679         04382605163141518161494337
3680 sage: t = p + 1 - r 490
3681 sage: t.nbits() 491
3682 129 492
3683 sage: abs(RR(t)) <= 2*sqrt(RR(p)) 493
3684 True 494
```

3685 **The  $j$ -invariant** As we have seen in XXX, [two elliptic curves  \$E\_1\(\mathbb{F}\)\$  defined by  \$y^2 = x^3 + ax + b\$](#)   
3686 [and  \$E\_2\(\mathbb{F}\)\$  defined by  \$y^2 + a'x + b'\$  are strictly isomorphic if and only if there is a quadratic](#)  
3687 [residue  \$d \in \mathbb{F}\$  such that  \$a' = ad^2\$  and  \$b' = bd^3\$ .](#)

add refer-  
ence

3688 There is, however, a more general way to classify elliptic curves over finite fields  $\mathbb{F}_q$ , based  
3689 on the so-called  **$j$ -invariant** of an elliptic curve with  $j(E(\mathbb{F}_q)) \in \mathbb{F}_q$ , as defined below:

$$j(E(\mathbb{F}_q)) = (1728 \bmod q) \frac{4 \cdot a^3}{4 \cdot a^3 + (27 \bmod q) \cdot b^2} \quad (5.31)$$

3690 A detailed description of the  $j$ -invariant is beyond the scope of this book. For our present  
3691 purposes, it is sufficient to note that two elliptic curves  $E_1(\mathbb{F})$  and  $E_2(\mathbb{F}')$  are isomorphic over  
3692 the **algebraic closures** of  $\mathbb{F}$  and  $\mathbb{F}'$ , if and only if  $\overline{\mathbb{F}} = \overline{\mathbb{F}'}$  and  $j(E_1) = j(E_2)$ .

algebraic  
closures

3693 So, the  $j$ -invariant is an important tool to classify elliptic curves and it is needed in the com-  
3694 plex multiplication method to decide on an actual curve instantiation that implements abstractly  
3695 chosen properties.

*Example 100.* Consider the elliptic curve  $E_1(\mathbb{F}_5)$  from example 68. [We compute its  \$j\$ -invariant](#) as follows:

check  
reference

$$\begin{aligned} j(E_1(\mathbb{F}_5)) &= (1728 \bmod 5) \frac{4 \cdot 1^3}{4 \cdot 1^3 + (27 \bmod 5) \cdot 1^2} \\ &= 3 \frac{4}{4 + 2} \\ &= 3 \cdot 4 = 2 \end{aligned}$$

*Example 101.* Consider the elliptic curve *TJJ\_13* from example 69. We compute its *j*-invariant as follows:

check  
reference

$$\begin{aligned}
 j(E_1(\mathbb{F}_5)) &= (1728 \bmod 13) \frac{4 \cdot 8^3}{4 \cdot 8^3 + (27 \bmod 13) \cdot 8^2} \\
 &= 12 \cdot \frac{4 \cdot 5}{4 \cdot 5 + 1 \cdot 12} \\
 &= 12 \cdot \frac{7}{7 + 12} \\
 &= 12 \cdot 7 \cdot 6^{-1} \\
 &= 12 \cdot 7 \cdot 11 \\
 &01
 \end{aligned}$$

*Example 102.* Consider *Secp256k1* from example *Secp256k1*. We compute its *j*-invariant using Sage:

check  
reference

```

3698 sage: p = 1157920892373161954235709850086879078532699846656405 495
3699      64039457584007908834671663
3700 sage: F = GF(p) 496
3701 sage: j = F(1728) * ( (F(4) * F(0) ^3) / (F(4) * F(0) ^3 + F(27) * F(7) ^2) ) 497
3702 sage: j == F(0) 498
3703 True 499

```

**The Complex Multiplication Method** As we have seen in the previous sections, elliptic curves have various defining properties, like their order, their prime factors, the embedding degree, or the cardinality (number of elements) of the base field. The **complex multiplication** (CM) method provides a practical way of constructing elliptic curves with pre-defined restrictions on the order and the base field.

The method usually starts by choosing a base field  $\mathbb{F}_q$  of the curve  $E(\mathbb{F}_q)$  we want to construct such that  $q = p^m$  for some prime number  $p$ , and “ $m \in \mathbb{N}$  with  $m \geq 1$ . We assume  $p > 3$  to simplify things in what follows.

Next, the trace of Frobenius  $t \in \mathbb{Z}$  of the curve is chosen such that  $p$  and  $t$  are coprime, that is,  $\gcd(p, t) = 1$  holds true. The choice of  $t$  also defines the curve’s order  $r$ , since  $r = p + 1 - t$  by the Hasse bound (equation 5.29), so choosing  $t$  will define the large order subgroup as well as all small cofactors.  $r$  has to be defined in such a way that the elliptic curve meets the security requirements of the application it is designed for.

check  
reference

Note that the choice of  $p$  and  $t$  also determines the embedding degree  $k$  of any prime-order subgroup of the curve, since  $k$  is defined as the smallest number such that the prime order  $n$  divides the number  $q^k - 1$ .

$$\begin{aligned}
 D &< 0 \\
 D \bmod 4 &= 0 \text{ or } D \bmod 4 = 1 \\
 4q &= t^2 + |D|v^2
 \end{aligned} \tag{5.32}$$

In order for the complex multiplication method to work, neither  $q$  nor  $t$  can be arbitrary, but must be chosen in such a way that two additional integers  $D \in \mathbb{Z}$  and  $v \in \mathbb{Z}$  exist and the following conditions hold:

If such numbers exist, we call  $D$  the **CM-discriminant**, and we know that we can construct a curve  $E(\mathbb{F}_q)$  over a finite field  $\mathbb{F}_q$  such that the order of the curve is  $|E(\mathbb{F}_q)| = q + 1 - t$ .

It is the content of the complex multiplication method to actually construct such a curve, that is finding the parameters  $a$  and  $b$  from  $\mathbb{F}_q$  in the defining Weierstraß equation such that the curve has the desired order  $r$ .

Finding solutions to equation 5.29, can be achieved in different ways, but we will forego the fine detail here. In general, it can be said that there are well-known constraints for elliptic curve families (e.g. the BLS (ECT) families) that provides families of solutions. In what follows, we will look at one type curve in the BLS-family, which gives an entire range of solutions. Are we looking at a subtype of BLS or is BLS the specific type we're referring to?

check  
reference

disambiguate

Assuming that the proper parameters  $q$ ,  $t$ ,  $D$  and  $v$  are found, we have to compute the so-called **Hilbert class polynomial**  $H_D \in \mathbb{Z}[x]$  of the CM-discriminant  $D$ , which is a polynomial with integer coefficients. To do so, we first have to compute the following set:

$$ICG(D) = \{(A, B, C) \mid A, B, C \in \mathbb{Z}, D = B^2 - 4AC, \gcd(A, B, C) = 1,$$

$$|B| \leq A \leq \sqrt{\frac{|D|}{3}}, A \leq C, \text{ if } B < 0 \text{ then } |B| < A < C\}$$

One way to compute this set is to first compute the integer  $A_{\max} = \text{Floor}(\sqrt{\frac{|D|}{3}})$ , then loop through all the integers  $A$  in the range  $[0, \dots, A_{\max}]$ , as well as through all the integers  $B$  in the range  $[-A_{\max}, \dots, A_{\max}]$ , then see if there is an integer  $C$  that satisfies  $D = B^2 - 4AC$  and the rest of the requirements in XXX.

To compute the Hilbert class polynomial, the so-called  **$j$ -function** (or  $j$ -invariant) is needed, which is a complex function defined on the upper half  $\mathbb{H}$  of the complex plane  $\mathbb{C}$ , usually written as follows: is this the same as equation eq:j-invariant1 No they just sound very similar. But they are very different?

add refer-  
enceunify ter-  
minology

$$j : \mathbb{H} \rightarrow \mathbb{C} \quad (5.33)$$

Roughly speaking, what this means is that the  $j$ -functions takes complex numbers  $(x + i \cdot y)$  with a positive imaginary part  $y > 0$  as inputs and returns a complex number  $j(x + i \cdot y)$  as a result.

For the purposes of this book, it is not important to understand the  $j$ -function in detail, and we can use Sage to compute it in a similar way that we would use Sage to compute any other well-known function. It should be noted, however, that the computation of the  $j$ -function in Sage is sometimes prone to precision errors. For example, the  $j$ -function has a root in  $\frac{-1+i\sqrt{3}}{2}$ , which Sage only approximates. Therefore, when using Sage to compute the  $j$ -function, we need to take precision loss into account and possibly round to the nearest integer.

```
sage: z = ComplexField(100) (0, 1) 500
sage: z # (0+1i) 501
1.00000000000000000000000000000000*I 502
sage: elliptic_j(z) 503
1728.000000000000000000000000000000 504
sage: # j-function only defined for positive imaginary 505
arguments
sage: z = ComplexField(100) (1, -1) 506
sage: try: 507
.....:     elliptic_j(z) 508
.....: except PariError: 509
```



```

3761     ....:         pass
3762 sage: # root at (-1+i sqrt(3))/2
3763 sage: z = ComplexField(100)(-1, sqrt(3))/2
3764 sage: elliptic_j(z)
3765 -2.6445453750358706361219364880e-88
3766 sage: elliptic_j(z).imag().round()
3767 0
3768 sage: elliptic_j(z).real().round()
3769 0

```

3770 With a way to compute the  $j$ -function and the precomputed set  $ICG(D)$  at hand, we can now  
 3771 compute the Hilbert class polynomial as follows:

$$H_D(x) = \prod_{(A,B,C) \in ICG(D)} \left( x - j \left( \frac{-B + \sqrt{D}}{2A} \right) \right) \quad (5.34)$$

3772 In other words, we loop over all elements  $(A, B, C)$  from the set  $ICG(D)$  and compute the  
 3773  $j$ -function at the point  $\frac{-B + \sqrt{D}}{2A}$ , where  $D$  is the CM-discriminant that we chose in a previous  
 3774 step. The result defines a factor of the Hilbert class polynomial and all factors are multiplied  
 3775 together.

3776 It can be shown that the Hilbert class polynomial is an integer polynomial, but actual com-  
 3777 putations need high-precision arithmetics to avoid approximation errors that usually occur in  
 3778 computer approximations of the  $j$ -function (as shown above). So, in case the calculated Hilbert  
 3779 class polynomial does not have integer coefficients, we need to round the result to the nearest  
 3780 integer. Given that the precision we used was high enough, the result will be correct.

In the next step, we use the Hilbert class polynomial  $H_D \in \mathbb{Z}[x]$ , and project it to a poly-  
 nomial  $H_{D,q} \in \mathbb{F}_q[x]$  with coefficients in the base field  $\mathbb{F}_q$  as chosen in the first step. We do  
 this by simply computing the new coefficients as the old coefficients modulus  $p$ , that is, if  
 $H_D(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0$ , we compute the  $q$ -modulus of each coefficient  
 $\tilde{a}_j = a_j \bmod p$ , which defines the **projected Hilbert class polynomial** as follows:

$$H_{D,p}(x) = \tilde{a}_m x^m + \tilde{a}_{m-1} x^{m-1} + \dots + \tilde{a}_1 x + \tilde{a}_0$$

3781 We then search for roots of  $H_{D,p}$ , since every root  $j_0$  of  $H_{D,p}$  defines a family of elliptic curves  
 3782 over  $\mathbb{F}_q$ , which all have a  $j$ -invariant 5.31 or 5.33 equal to  $j_0$ . We can pick any root, since all of  
 3783 them will lead to proper curves eventually.

check  
reference

3784 However, some of the curves with the correct  $j$ -invariant might have an order different from  
 3785 the one we initially decided on. Therefore, we need a way to decide on a curve with the correct  
 3786 order.

3787 To compute such a curve, we have to distinguish a few different cases based on our choice  
 3788 of the root  $j_0$  and of the CM-discriminant  $D$ . If  $j_0 \neq 0$  or  $j_0 \neq 1728 \bmod q$ , we compute  
 3789  $c_1 = \frac{j_0}{(1728 \bmod q) - j_0}$ , then we chose some arbitrary quadratic non-residue  $c_2 \in \mathbb{F}_q$ , and some  
 3790 arbitrary cubic non-residue  $c_3 \in \mathbb{F}_q$ .

3791 The following table is guaranteed to define a curve with the correct order  $r = q + 1 - t$  for  
 3792 the trace of Frobenius  $t$  we initially decided on:

actually  
make this  
a table?

3793 **Definition 5.4.0.1.** • Case  $j_0 \neq 0$  and  $j_0 \neq 1728 \bmod q$ . A curve with the correct order is  
 3794 defined by one of the following equations:

$$y^2 = x^3 + 3c_1 x + 2c_1 \quad \text{or} \quad y^2 = x^3 + 3c_1 c_2^2 x + 2c_1 c_2^3 \quad (5.35)$$

3795

3796

- Case  $j_0 = 0$  and  $D \neq -3$ . A curve with the correct order is defined by one of the following equations:

$$y^2 = x^3 + 1 \quad \text{or} \quad y^2 = x^3 + c_2^3 \quad (5.36)$$

- Case  $j_0 = 0$  and  $D = -3$ . A curve with the correct order is defined by one of the following equations:

$$\begin{aligned} y^2 &= x^3 + 1 \quad \text{or} \quad y^2 = x^3 + c_2^3 \quad \text{or} \\ y^2 &= x^3 + c_3^2 \quad \text{or} \quad y^2 = c_3^2 c_2^3 \quad \text{or} \\ y^2 &= x^3 + c_3^{-2} \quad \text{or} \quad y^2 = x^3 + c_3^{-2} c_2^3 \end{aligned}$$

3797

3798

- Case  $j_0 = 1728 \bmod q$  and  $D \neq -4$ . A curve with the correct order is defined by one of the following equations:

$$y^2 = x^3 + x \quad \text{or} \quad y^2 = x^3 + c_2^2 x \quad (5.37)$$

- Case  $j_0 = 1728 \bmod q$  and  $D = -4$ . A curve with the correct order is defined by one of the following equations:

$$\begin{aligned} y^2 &= x^3 + x \quad \text{or} \quad y^2 = x^3 + c_2 x \quad \text{or} \\ y^2 &= x^3 + c_2^2 x \quad \text{or} \quad y^2 = x^3 + c_2^3 x \end{aligned}$$

3799

3800

3801

3802

3803

To decide the proper defining Weierstraß equation, we therefore have to compute the order of any of the potential curves above, and then choose the one that fits our initial requirements. Since it can be shown that the Hilbert class polynomials for the CM-discriminants  $D = -3$  and  $D = -4$  are given by  $H_{-3,q}(x) = x$  and  $H_{-4,q}(x) = x - (1728 \bmod q)$  (EXERCISE), the previous cases are exhaustive.

3804

3805

3806

3807

3808

3809

3810

3811

3812

3813

To summarize, using the complex multiplication method, it is possible to synthesize elliptic curves with predefined order over predefined base fields from scratch. However, the curves that are constructed this way are just some representatives of a larger class of curves, all of which have the same order. Therefore, in real-world applications, it is sometimes more advantageous to choose a different representative from that class. To do so recall from XXX that any curve defined by the Weierstraß equation  $y^2 = x^3 + ax + b$  is isomorphic to a curve of the form  $y^2 = x^3 + ad^2x + bd^3$  for some quadratic residue  $d \in \mathbb{F}_q$ .

In order to find a suitable representative (e.g. with small parameters  $a$  and  $b$ ) in the last step, the curve designer might choose a quadratic residue  $d$  such that the transformed curve has the properties they wanted.

3814

3815

3816

3817

*Example 103.* Consider curve  $E_1(\mathbb{F}_5)$  from example 68. We want to use the complex multiplication method to derive that curve from scratch. Since  $E_1(\mathbb{F}_5)$  is a curve of order  $r = 9$  over the prime field of order  $q = 5$ , we know from example 97 that its trace of Frobenius is  $t = -3$ , which also implies that  $q$  and  $|t|$  are coprime.

We then have to find parameters  $D, v \in \mathbb{Z}$  such that the criteria in 5.32 hold. We get the following:

$$\begin{aligned} 4q &= t^2 + |D|v^2 && \Rightarrow \\ 20 &= (-3)^2 + |D|v^2 && \Leftrightarrow \\ 11 &= |D|v^2 \end{aligned}$$

exercise  
still to be  
written?

add refer-  
ence

check  
reference

check  
reference



Now, since 11 is a prime number, the only solution is  $|D| = 11$  and  $v = 1$  here. With  $D = -11$  and the Euclidean division of  $-11$  by 4 being  $-11 = -3 \cdot 4 + 1$ , we have  $-11 \bmod 4 = 1$ , which shows that  $D = -11$  is a proper choice.

In the next step, we have to compute the Hilbert class polynomial  $H_{-11}$ . To do so, we first have to find the set  $ICG(D)$ . To compute that set, observe that, since  $\sqrt{\frac{|D|}{3}} \approx 1.915 < 2$ , we know from  $A \leq \sqrt{\frac{|D|}{3}}$  and  $A \in \mathbb{Z}$  that  $A$  must be either 0 or 1.

For  $A = 0$ , we know  $B = 0$  from the constraint  $|B| \leq A$ . However, in this case, there could be no  $C$  satisfying  $-11 = B^2 - 4AC$ . So we try  $A = 1$  and deduce  $B \in \{-1, 0, 1\}$  from the constraint  $|B| \leq A$ . The case  $B = -1$  can be excluded, since then  $B < 0$  has to imply  $|B| < A$ . The case  $B = 0$  can also be excluded, as there cannot be an integer  $C$  with  $-11 = -4C$ , since 11 is a prime number.

This leaves the case  $B = 1$ , and we compute  $C = 3$  from the equation  $-11 = 1^2 - 4C$ , which gives the solution  $(A, B, C) = (1, 1, 3)$ :

$$ICG(D) = \{(1, 1, 3)\}$$

With the set  $ICG(D)$  at hand, we can compute the Hilbert class polynomial of  $D = -11$ . To do so, we have to insert the term  $\frac{-1+\sqrt{-11}}{2}$  into the  $j$ -function. To do so, first observe that  $\sqrt{-11} = i\sqrt{11}$ , where  $i$  is the imaginary unit, defined by  $i^2 = -1$ . Using this, we can invoke Sage to compute the  $j$ -invariant and get the following:

$$H_{-11}(x) = x - j\left(\frac{-1+i\sqrt{11}}{2}\right) = x + 32768$$

As we can see, in this particular case, the Hilbert class polynomial is a linear function with a single integer coefficient. In the next step, we have to project it onto a polynomial from  $\mathbb{F}_5[x]$  by computing the modular 5 remainder of the coefficients 1 and 32768. We get  $32768 \bmod 5 = 3$ , from which it follows that the projected Hilbert class polynomial is considered a polynomial from  $\mathbb{F}_5[x]$ :

$$H_{-11,5}(x) = x + 3$$

As we can see, the only root of this polynomial is  $j = 2$ , since  $H_{-11,5}(2) = 2 + 3 = 0$ . We therefore have a situation with  $j \neq 0$  and  $j \neq 1728$ , which tells us that we have to compute the parameter  $c_1$  in modular 5 arithmetics:

$$c_1 = \frac{2}{1728 - 2}$$

Since  $1728 \bmod 5 = 3$ , we get  $c_1 = 2$ .

Next, we have to check if the curve  $E(\mathbb{F}_5)$  defined by the Weierstraß equation  $y^2 = x^3 + 3 \cdot 2x + 2 \cdot 2$  has the correct order. We invoke Sage, and find that the order is indeed 9, so it is a curve with the required parameters. Thus, we have successfully constructed the curve with the desired properties.

Note, however, that in real-world applications, it might be useful to choose parameters  $a$  and  $b$  that have certain properties, e.g. to be as small as possible. As we know from XXX, choosing any quadratic residue  $d \in \mathbb{F}_5$  gives a curve of the same order defined by  $y^2 = x^2 + ak^2x + bk^3$ . Since 4 is a quadratic residue in  $\mathbb{F}_4$ , we can transform the curve defined by  $y^2 = x^3 + x + 4$  into the curve  $y^2 = x^3 + 4^2 + 4 \cdot 4^3$  which gives the following:

$$y^2 = x^3 + x + 1$$

add reference

3834 This is the curve  $E_1(\mathbb{F}_5)$  that we used extensively throughout this book. Thus, using the  
 3835 complex multiplication method, we were able to derive a curve with specific properties from  
 3836 scratch.

3837 *Example 104.* Consider the tiny-jubjub curve  $TJJ\_13$  from example 69. We want to use the  
 3838 complex multiplication method to derive that curve from scratch. Since  $TJJ\_13$  is a curve of  
 3839 order  $r = 20$  over the prime field of order  $q = 13$ , we know from example 98 that its trace of  
 3840 Frobenius is  $t = -6$ , which also implies that  $q$  and  $|t|$  are coprime.

check  
referencecheck  
reference

We then have to find parameters  $D, v \in \mathbb{Z}$  such that 5.32 holds. We get the following:

$$\begin{aligned} 4q &= t^2 + |D|v^2 && \Rightarrow \\ 4 \cdot 13 &= (-6)^2 + |D|v^2 && \Rightarrow \\ 52 &= 36 + |D|v^2 && \Leftrightarrow \\ 16 &= |D|v^2 \end{aligned}$$

3841 This equation has two solutions for  $(D, v)$ , namely  $(-4, \pm 2)$  and  $(-16, \pm 1)$ . Looking at the  
 3842 first solution, we know that  $D = -4$  implies  $j = 1728$ , and the constructed curve is defined by  
 3843 a Weierstraß equation 5.1 that has a vanishing parameter  $b = 0$ . We can therefore conclude that  
 3844 choosing  $D = -4$  will not help us reconstructing  $TJJ\_13$ . It will produce curves with order 20,  
 3845 just not the one we are looking for.

check  
reference

So we choose the second solution  $D = -16$ . In the next step, we have to compute the Hilbert class polynomial  $H_{-16}$ . To do so, we first have to find the set  $ICG(D)$ . To compute that set, observe that since  $\sqrt{\frac{|-16|}{3}} \approx 2.31 < 3$ , we know from  $A \leq \sqrt{\frac{|-16|}{3}}$  and  $A \in \mathbb{Z}$  that  $A$  must be in the range  $0..2$ . So we loop through all possible values of  $A$  and through all possible values of  $B$  under the constraints  $|B| \leq A$ , and if  $B < 0$  then  $|B| < A$ . Then we compute potential  $C$ 's from  $-16 = B^2 - 4AC$ . We get the following two solutions for  $ICG(D)$ : we get

$$ICG(D) = \{(1, 0, 4), (2, 0, 2)\}$$

With the set  $ICG(D)$  at hand, we can compute the Hilbert class polynomial of  $D = -16$ . We can invoke Sage to compute the  $j$ -invariant and get the following:

$$\begin{aligned} H_{-16}(x) &= \left( x - j \left( \frac{i\sqrt{16}}{2} \right) \right) \left( x - j \left( \frac{i\sqrt{16}}{4} \right) \right) \\ &= (x - 287496)(x - 1728) \end{aligned}$$

As we can see, in this particular case, the Hilbert class polynomial is a quadratic function with two integer coefficients. In the next step, we have to project it onto a polynomial from  $\mathbb{F}_5[x]$  by computing the modular 5 remainder of the coefficients 1, 287496 and 1728. We get  $287496 \bmod 13 = 1$  and  $1728 \bmod 13 = 2$ , which means that the projected Hilbert class polynomial is as follows:

$$H_{-11,5}(x) = (x - 1)(x - 12) = (x + 12)(x + 1)$$

3846 This is considered a polynomial from  $\mathbb{F}_5[x]$ . Thus, we have two roots, namely  $j = 1$  and  $j =$   
 3847 12. We already know that  $j = 12$  is the wrong root to construct the tiny-jubjub curve, since  
 3848  $1728 \bmod 13 = 2$ , and that case is not compatible with a curve with  $b \neq 0$ . So we choose  $j = 1$ .

Another way to decide the proper root is to compute the  $j$ -invariant of the tiny-jubjub curve. We get the following:

$$\begin{aligned}
 j(TJJ\_13) &= 12 \frac{4 \cdot 8^3}{4 \cdot 8^3 + 1 \cdot 8^2} \\
 &= 12 \frac{4 \cdot 5}{4 \cdot 5 + 12} \\
 &= 12 \frac{7}{7 + 12} \\
 &= 12 \frac{7}{7 + 12} \\
 &= 1
 \end{aligned}$$

This is equal to the root  $j = 1$  of the Hilbert class polynomial  $H_{-16,13}$  as expected. We therefore have a situation with  $j \neq 0$  and  $j \neq 1728$ , which tells us that we have to compute the parameter  $c_1$  in modular 5 arithmetics:

$$c_1 = \frac{1}{12 - 1} = 6$$

Since  $1728 \bmod 13 = 12$ , we get  $c_1 = 6$ . Then we have to check if the curve  $E(\mathbb{F}_5)$  defined by the Weierstraß equation  $y^2 = x^3 + 3 \cdot 6x + 2 \cdot 6$ , which is equivalent to  $y^2 = x^3 + 5x + 12$ , has the correct order. We invoke Sage and find that the order is 8, which implies that the trace of this curve is 6, not  $-6$  as required. So we have to consider the second possibility, and choose some quadratic non-residue  $c_2 \in \mathbb{F}_{13}$ . We choose  $c_2 = 5$  and compute the Weierstraß equation  $y^2 = x^3 + 5c_2^2 + 12c_2^3$  as follows:

$$y^2 = x^3 + 8x + 5$$

We invoke Sage and find that the order is 20, which is indeed the correct one. As we know from XXX, choosing any quadratic residue  $d \in \mathbb{F}_5$  gives a curve of the same order defined by  $y^2 = x^2 + ad^2x + bd^3$ . Since 12 is a quadratic residue in  $\mathbb{F}_{13}$ , we can transform the curve defined by  $y^2 = x^3 + 8x + 5$  into the curve  $y^2 = x^3 + 12^2 \cdot 8 + 5 \cdot 12^3$  which gives the following:

$$y^2 = x^3 + 8x + 8$$

add reference

3849 This is the tiny-jubjub curve that we used extensively throughout this book. So using the  
3850 complex multiplication method, we were able to derive a curve with specific properties from  
3851 scratch.

*Example 105.* To consider a real-world example, we want to use the complex multiplication method in combination with Sage to compute Secp256k1 from scratch. So based on example 70, we decided to compute an elliptic curve over a prime field  $\mathbb{F}_p$  of order  $r$  for the following security parameters:

check reference

$$\begin{aligned}
 p &= 115792089237316195423570985008687907853269984665640564039457584007908834671663 \\
 r &= 115792089237316195423570985008687907852837564279074904382605163141518161494337
 \end{aligned}$$

According to example 99, this gives the following trace of Frobenius:

check reference

$$t = 4324203865659659652420866390673177327$$

3852 We also decided that we want a curve of the form  $y^2 = x^3 + b$ , that is, we want the parameter  
3853  $a$  to be zero. This implies that the  $j$ -invariant of our curve must be zero.

In a first step, we have to find a CM-discriminant  $D$  and some integer  $v$  such that the equation  $4p = t^2 + |D|v^2$  is satisfied. Since we aim for a vanishing  $j$ -invariant, the first thing to try is  $D = -3$ . In this case, we can compute  $v^2 = (4p - t^2)$ , and if  $v^2$  happens to be an integer that has a square root  $v$ , we are done. Invoking Sage we compute as follows:

```

3854 sage: D = -3
3855 sage: p = 1157920892373161954235709850086879078532699846656405
3856 sage: r = 1157920892373161954235709850086879078528375642790749
3857 sage: t = p+1-r
3858 sage: v_sqr = (4*p - t^2)/abs(D)
3859 sage: v_sqr.is_integer()
3860 True
3861 sage: v = sqrt(v_sqr)
3862 sage: v.is_integer()
3863 True
3864 sage: 4*p == t^2 + abs(D)*v^2
3865 True
3866 sage: v
3867 303414439467246543595250775667605759171

```

The pair  $(D, v) = (-3, 303414439467246543595250775667605759171)$  does indeed solve the equation, which tells us that there is a curve of order  $r$  over a prime field of order  $p$ , defined by a Weierstraß equation  $y^2 = x^3 + b$  for some  $b \in \mathbb{F}_p$ . Now we need to compute  $b$ .

For  $D = -3$ , we already know that the associated Hilbert class polynomial is given by  $H_{-3}(x) = x$ , which gives the projected Hilbert class polynomial as  $H_{-3,p} = x$  and the  $j$ -invariant of our curve is guaranteed to be  $j = 0$ . Now, looking at 5.4.0.1, we see that there are 6 possible cases to construct a curve with the correct order  $r$ . In order to construct the curves in question, we have to choose some arbitrary quadratic and cubic non-residue. So we loop through  $\mathbb{F}_p$  to find them, invoking Sage:

```

3883 sage: F = GF(p)
3884 sage: for c2 in F:
3885     try: # quadratic residue
3886         _ = c2.nth_root(2)
3887     except ValueError: # quadratic non-residue
3888         break
3889 sage: c2
3890 3
3891 sage: for c3 in F:
3892     try:
3893         _ = c3.nth_root(3)
3894     except ValueError:
3895         break
3896 sage: c3
3897 2

```

We found the quadratic non-residue  $c_2 = 3$  and the cubic non-residue  $c_3 = 2$ . Using those numbers, we check the six cases against the the expected order  $r$  of the curve we want to

check  
reference

3900 synthesize:

```

3901 sage: C1 = EllipticCurve(F, [0, 1])           548
3902 sage: C1.order() == r                         549
3903 False                                         550
3904 sage: C2 = EllipticCurve(F, [0, c2^3])        551
3905 sage: C2.order() == r                         552
3906 False                                         553
3907 sage: C3 = EllipticCurve(F, [0, c3^2])        554
3908 sage: C3.order() == r                         555
3909 False                                         556
3910 sage: C4 = EllipticCurve(F, [0, c3^2*c2^3])   557
3911 sage: C4.order() == r                         558
3912 False                                         559
3913 sage: C5 = EllipticCurve(F, [0, c3^(-2)])      560
3914 sage: C5.order() == r                         561
3915 False                                         562
3916 sage: C6 = EllipticCurve(F, [0, c3^(-2)*c2^3]) 563
3917 sage: C6.order() == r                         564
3918 True                                          565

```

As expected, we found an elliptic curve of the correct order  $r$  over a prime field of size  $p$ . In principle, we are done, as we have found a curve with the same basic properties as Secp256k1. However, the curve is defined by the following equation, which uses a very large parameter  $b_1$ , and so it might perform too slowly in certain algorithms.

$$y^2 = x^3 + 86844066927987146567678238756515930889952488499230423029593188005931626003754x$$

It is also not very elegant to be written down by hand. It might therefore be advantageous to find an isomorphic curve with the smallest possible parameter  $b_2$ . In order to find such a  $b_2$ , we have to choose a quadratic residue  $d$  such that  $b_2 = b_1 \cdot d^3$  is as small as possible. To do so, we rewrite the last equation into the following form:

$$d = \sqrt[3]{\frac{b_2}{b_1}}$$

what does this mean? Maybe just delete it

3919 Then we invoke Sage to loop through values  $b_2 \in \mathbb{F}_p$  until it finds some number such that  
 3920 the quotient  $\frac{b_2}{b_1}$  has a cube root  $d$  and this cube root itself is a quadratic residue.

```

3921 sage: b1=86844066927987146567678238756515930889952488499230423  566
3922       029593188005931626003754
3923 sage: for b2 in F:                                           567
3924     ....:     try:                                           568
3925     ....:         d = (b2/b1).nth_root(3)                   569
3926     ....:         try:                                       570
3927     ....:             _ = d.nth_root(2)                     571
3928     ....:             if d != 0:                             572
3929     ....:                 break                               573
3930     ....:         except ValueError:                          574
3931     ....:             pass                                    575
3932     ....:     except ValueError:                              576
3933     ....:         pass                                        577

```

3934 **sage: b2**  
 3935 **7**

578

579

3936 Indeed, the smallest possible value is  $b_2 = 7$  and the defining Weierstraß equation of a curve  
 3937 over  $\mathbb{F}_p$  with prime order  $r$  is  $y^2 = x^3 + 7$ , which we might call Secp256k1. As we have just  
 3938 seen, the complex multiplication method is powerful enough to derive cryptographically secure  
 3939 curves like Secp256k1 from scratch.

3940 **The BLS6\_6 pen-and-paper curve** In this paragraph, we summarize our understanding of  
 3941 elliptic curves to derive our main pen-and-paper example for the rest of the book. To do so, we  
 3942 want to use the complex multiplication method to derive a pairing-friendly elliptic curve that  
 3943 has similar properties to curves that are used in actual cryptographic protocols. However, we  
 3944 design the curve specifically to be useful in pen-and-paper examples, which mostly means that  
 3945 the curve should contain only a few points so that we are able to derive exhaustive addition and  
 3946 pairing tables.

3947 A well-understood family of pairing-friendly curves is the the group of BLS curves (STUFF  
 3948 ABOUT THE HISTORY AND THE NAMING CONVENTION), which are derived in [XXX].  
 3949 BLS curves are particularly useful in our case if the embedding degree  $k$  satisfies  $k \equiv 6 \pmod{0}$ .  
 3950 Of course, the smallest embedding degree  $k$  that satisfies this congruency is  $k = 6$  and we there-  
 3951 fore aim for a BLS6 curve as our main pen-and-paper example.

write up  
this part

add refer-  
ence

3952 To apply the complex multiplication method from page 113 ff., recall that this method starts  
 3953 with a definition of the base field  $\mathbb{F}_{p^m}$ , as well as the trace of Frobenius  $t$  and the order of the  
 3954 curve. If the order  $p^m + 1 - t$  is not a prime number, then the order  $r$  of the largest prime factor  
 3955 group needs to be controlled.

check  
reference

3956 In the case of BLS\_6 curves, the parameter  $m$  is chosen to be 1, which means that the  
 3957 curves are defined over prime fields. All relevant parameters  $p$ ,  $t$  and  $r$  are then themselves  
 3958 parameterized by the following three polynomials:

$$\begin{aligned} r(x) &= \Phi_6(x) \\ t(x) &= x + 1 \\ q(x) &= \frac{1}{3}(x-1)^2(x^2 - x + 1) + x \end{aligned} \tag{5.38}$$

3959 In the equations above,  $\Phi_6$  is the 6-th cyclotomic polynomial and  $x \in \mathbb{N}$  is a parameter  
 3960 that the designer has to choose in such a way that the evaluation of  $p$ ,  $t$  and  $r$  at the point  $x$   
 3961 gives integers that have the proper size to meet the security requirements of the curve that they  
 3962 want to design. It is then guaranteed that the complex multiplication method can be used in  
 3963 combination with those parameters to define an elliptic curve with CM-discriminant  $D = -3$ ,  
 3964 embedding degree  $k = 6$ , and curve equation  $y^2 = x^3 + b$  for some  $b \in \mathbb{F}_p$ .

cyclotomic  
polyno-  
mial

3965 For example, if the curve should target the 128-bit security level, due to the Pholaard-rho  
 3966 attack (TODO) the parameter  $r$  should be prime number of at least 256 bits.

Pholaard-  
rho attack

3967 In order to design the smallest BLS\_6 curve, we therefore have to find a parameter  $x$  such  
 3968 that  $r(x)$ ,  $t(x)$  and  $q(x)$  are the smallest natural numbers that satisfy  $q(x) > 3$  and  $r(x) > 3$ .<sup>1</sup>

todo

We therefore initiate the design process of our BLS6 curve by looking up the 6-th cyclo-  
 tomic polynomial, which is  $\Phi_6 = x^2 - x + 1$ , and then insert small values for  $x$  into the defining

<sup>1</sup>The smallest BLS curve will also be the most insecure BLS curve. However, since our goal with this curve is ease of pen-and-paper computation rather than security, it fits the purposes of this book.



polynomials  $r, t, q$ . We get the following results:

$$\begin{array}{lll} x = 1 & (r(x), t(x), q(x)) & (1, 2, 1) \\ x = 2 & (r(x), t(x), q(x)) & (3, 3, 3) \\ x = 3 & (r(x), t(x), q(x)) & (7, 4, \frac{37}{3}) \\ x = 4 & (r(x), t(x), q(x)) & (13, 5, 43) \end{array}$$

Since  $q(1) = 1$  is not a prime number, the first  $x$  that gives a proper curve is  $x = 2$ . However, such a curve would be defined over a base field of characteristic 3, and we would rather like to avoid that. We therefore find  $x = 4$ , which defines a curve over the prime field of characteristic 43 that has a trace of Frobenius  $t = 5$  and a larger order prime group of size  $r = 13$ .

Since the prime field  $\mathbb{F}_{43}$  has 43 elements and 43's binary representation is  $43_2 = 101011$ , which consists of 6 digits, the name of our pen-and-paper curve should be *BLS6\_6*, since its is common to name a BLS curve by its embedding degree and the bit-length of the modulus in the base field. We call *BLS6\_6* the **moon-math-curve**.

Based on 5.29, we know that the Hasse bound implies that *BLS6\_6* will contain exactly 39 elements. Since the prime factorization of 39 is  $39 = 3 \cdot 13$ , we have a “large” prime factor group of size 13, as expected, and a small cofactor group of size 3. Fortunately, a subgroup of order 13 is well suited for our purposes, as 13 elements can be easily handled in the associated addition, scalar multiplication and pairing tables in a pen-and-paper style.

We can check that the embedding degree is indeed 6 as expected, since  $k = 6$  is the smallest number  $k$  such that  $r = 13$  divides  $43^k - 1$ .

```
sage: for k in range(1, 42): # Fermat's little theorem
      ....:     if (43^k - 1) % 13 == 0:
      ....:         break
sage: k
6
```

In order to compute the defining equation  $y^2 = x^3 + ax + b$  of *BLS6\_6*, we use the complex multiplication method as described in 5.4. The goal is to find  $a, b \in \mathbb{F}_{43}$  representations that are particularly nice to work with. The authors of XXX showed that the CM-discriminant of every BLS curve is  $D = -3$  and, indeed, the following equation has the four solutions  $(D, v) \in \{(-3, -7), (-3, 7), (-49, -1), (-49, 1)\}$  if  $D$  is required to be negative, as expected:

$$\begin{aligned} 4p &= t^2 + |D|v^2 && \Rightarrow \\ 4 \cdot 43 &= 5^2 + |D|v^2 && \Rightarrow \\ 172 &= 25 + |D|v^2 && \Leftrightarrow \\ 49 &= |D|v^2 \end{aligned}$$

This means that  $D = -3$  is indeed a proper CM-discriminant, and we can deduce that the parameter  $a$  has to be 0, and that the Hilbert class polynomial is given by  $H_{-3, 43}(x) = x$ .

This implies that the  $j$ -invariant of *BLS6\_6* is given by  $j(\text{BLS6\_6}) = 0$ . We therefore have to look at case XXX in table 5.4.0.1 to derive a parameter  $b$ . To decide the proper case for  $j_0 = 0$  and  $D = -3$ , we therefore have to choose some arbitrary quadratic non-residue  $c_2$  and cubic non-residue  $c_3$  in  $\mathbb{F}_{43}$ . We choose  $c_2 = 5$  and  $c_3 = 36$ . We check these with Sage:

```
sage: F43 = GF(43)
```

why? Because in this book elliptic curves are only defined for fields of characteristic  $> 3$

check reference

580  
581  
582  
583  
584

check reference

what does this mean?

add reference

add reference

check reference

```

4001 sage: c2 = F43(5) 586
4002 ..... try: # quadratic residue 587
4003 ..... c2.nth_root(2) 588
4004 ..... except ValueError: # quadratic non-residue 589
4005 ..... c2 590
4006 sage: c3 = F43(36) 591
4007 ..... try: 592
4008 ..... c3.nth_root(3) 593
4009 ..... except ValueError: 594
4010 ..... c3 595

```

4011 Using those numbers we check the six possible cases from 5.4.0.1 against the the expected  
 4012 order 39 of the curve we want to synthesize:

check  
reference

```

4013 sage: BLS61 = EllipticCurve(F43, [0, 1]) 596
4014 sage: BLS61.order() == 39 597
4015 False 598
4016 sage: BLS62 = EllipticCurve(F43, [0, c2^3]) 599
4017 sage: BLS62.order() == 39 600
4018 False 601
4019 sage: BLS63 = EllipticCurve(F43, [0, c3^2]) 602
4020 sage: BLS63.order() == 39 603
4021 True 604
4022 sage: BLS64 = EllipticCurve(F43, [0, c3^2*c2^3]) 605
4023 sage: BLS64.order() == 39 606
4024 False 607
4025 sage: BLS65 = EllipticCurve(F43, [0, c3^(-2)]) 608
4026 sage: BLS65.order() == 39 609
4027 False 610
4028 sage: BLS66 = EllipticCurve(F43, [0, c3^(-2)*c2^3]) 611
4029 sage: BLS66.order() == 39 612
4030 False 613
4031 sage: BLS6 = BLS63 # our BLS6 curve in the book 614

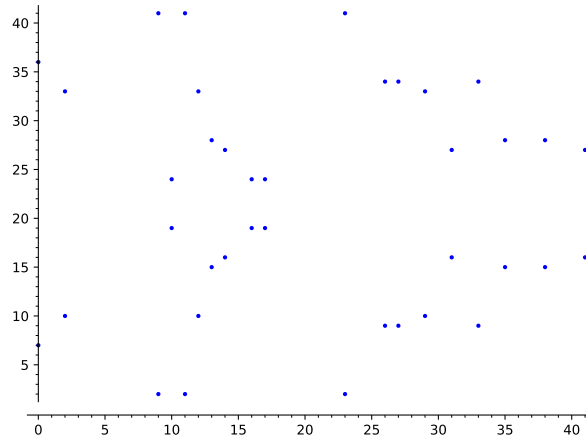
```

4032 As expected, we found an elliptic curve of the correct order 39 over a prime field of size 43,  
 4033 defined by the following equation:

$$BLS6\_6 := \{(x, y) \mid y^2 = x^3 + 6 \text{ for all } x, y \in \mathbb{F}_{43}\} \quad (5.39)$$

4034 There are other choices for  $b$ , such as  $b = 10$  or  $b = 23$ , but all these curves are isomorphic,  
 4035 and hence represent the same curve in a different way. Since BLS6-6 only contains 39 points, it  
 4036 is possible to give a visual impression of the curve:





4037

4038 As we can see, our curve has some desirable properties: it does not contain self-inverse  
 4039 points, that is, points with  $y = 0$ . It follows that the addition law can be optimized, since the  
 4040 branch for those cases can be eliminated.

4041 Summarizing the previous procedure, we have used the method of Barreto, Lynn and Scott  
 4042 to construct a pairing-friendly elliptic curve of embedding degree 6. However, in order to do  
 4043 elliptic curve cryptography on this curve, note that, since the order of  $BLS6\_6$  is 39, its group  
 4044 of rational points is not a finite cyclic group of prime order. We therefore have to find a suitable  
 4045 subgroup as our main target. Since  $39 = 13 \cdot 3$ , we know that the curve must contain a “large”  
 4046 prime-order group of size 13 and a small cofactor group of order 3.

4047 The following step is to construct this group. One way to do so is to find a generator. We  
 4048 can achieve this by choosing an arbitrary element of the group that is not the point at infinity,  
 4049 and then multiply that point with the cofactor of the group’s order. If the result is not the point  
 4050 at infinity, the result will be a generator. If it is the point at infinity we have to choose a different  
 4051 element.

In order to find a generator for the large order subgroup of size 13, we first notice that the cofactor of 13 is 3, since  $39 = 3 \cdot 13$ . We then need to construct an arbitrary element from  $BLS6\_6$ . To do so in a pen-and-paper style, we can choose some *arbitrary*  $x \in \mathbb{F}_{43}$  and see if there is some solution  $y \in \mathbb{F}_{43}$  that satisfies the defining Weierstraß equation  $y^2 = x^3 + 6$ . We choose  $x = 9$ , and check that  $y = 2$  is a proper solution:

$$\begin{aligned} y^2 &= x^3 + 6 && \Rightarrow \\ 2^2 &= 9^3 + 6 && \Leftrightarrow \\ 4 &= 4 \end{aligned}$$

4052 This implies that  $P = (9, 2)$  is therefore a point on  $BLS6\_6$ . To see if we can project this  
 4053 point onto a generator of the large order prime group  $BLS6\_6[13]$ , we have to multiply  $P$  with  
 4054 the cofactor, that is, we have to compute  $[3](9, 2)$ . After some computation (EXERCISE) we  
 4055 get  $[3](9, 2) = (13, 15)$ . Since this is not the point at infinity, we know that  $(13, 15)$  must be a  
 4056 generator of  $BLS6\_6[13]$ . The generator  $g_{BLS6\_6[13]}$ , which we will use in pairing computations  
 4057 in the remainder of this book, is given as follows:

$$g_{BLS6\_6[13]} = (13, 15) \tag{5.40}$$

4058 Since  $g_{BLS6\_6[13]}$  is a generator, we can use it to construct the subgroup  $BLS6\_6[13]$  by re-  
 4059 peatedly adding the generator to itself. Using Sage, we get the following:

4060 **sage:** `P = BLS6(9, 2)`

 add refer-  
ence

 add exer-  
cise

```

4061 sage: Q = 3*P 616
4062 sage: Q.xy() 617
4063 (13, 15) 618
4064 sage: BLS6_13 = [] 619
4065 sage: for x in range(0,13): # cyclic of order 13 620
4066     ....:     P = x*Q 621
4067     ....:     BLS6_13.append(P) 622

```

Repeatedly adding a generator to itself, as we just did, will generate small groups in logarithmic order with respect to the generator as, explained on page 43 ff. We therefore get the following description of the large prime-order subgroup of  $BLS6_6$ :

check  
reference

$$\begin{aligned}
 BLS6_6[13] = \\
 \{ (13, 15) \rightarrow (33, 34) \rightarrow (38, 15) \rightarrow (35, 28) \rightarrow (26, 34) \rightarrow (27, 34) \rightarrow \\
 (27, 9) \rightarrow (26, 9) \rightarrow (35, 15) \rightarrow (38, 28) \rightarrow (33, 9) \rightarrow (13, 28) \rightarrow \mathcal{O} \} \quad (5.41)
 \end{aligned}$$

Having a logarithmic description of this group is tremendously helpful in pen-and-paper computations. To see that, observe that we know from XXX that there is an exponential map from the scalar field  $\mathbb{F}_{13}$  to  $BLS6_6[13]$  with respect to our generator, which generates the group in logarithmic order:

add refer-  
ence

$$[\cdot]_{(13,15)} : \mathbb{F}_{13} \rightarrow BLS6_6[13] ; x \mapsto [x](13, 15)$$

So, for example, we have  $[1]_{(13,15)} = (13, 15)$ ,  $[7]_{(13,15)} = (27, 9)$  and  $[0]_{(13,15)} = \mathcal{O}$  and so on. The relevant point here is that we can use this representation to do computations in  $BLS6_6[13]$  efficiently in our head using XXX, as in the following example:

add refer-  
ence

$$\begin{aligned}
 (27, 34) \oplus (33, 9) &= [6](13, 15) \oplus [11](13, 15) \\
 &= [6 + 11](13, 15) \\
 &= [4](13, 15) \\
 &= (35, 28)
 \end{aligned}$$

So XXX is really all we need to do computations in  $BLS6_6[13]$  in this book efficiently. However, out of convenience, the following picture lists the entire addition table of that group, as it might be useful in pen-and-paper computations:

add refer-  
ence

$\oplus$	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)	(35, 28)	(26, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)	(13, 28)
$\mathcal{O}$	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)	(35, 28)	(26, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)	(13, 28)
(13, 15)	(13, 15)	(33, 34)	(38, 15)	(35, 28)	(26, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)	(13, 28)	$\mathcal{O}$
(33, 34)	(33, 34)	(38, 15)	(35, 28)	(26, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)	(13, 28)	$\mathcal{O}$	(13, 15)
(38, 15)	(38, 15)	(35, 28)	(26, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)	(13, 28)	$\mathcal{O}$	(13, 15)	(33, 34)
(35, 28)	(35, 28)	(26, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)	(13, 28)	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)
(26, 34)	(26, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)	(13, 28)	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)	(35, 28)
(27, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)	(13, 28)	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)	(35, 28)	(26, 34)
(27, 9)	(27, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)	(13, 28)	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)	(35, 28)	(26, 34)	(27, 34)
(26, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)	(13, 28)	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)	(35, 28)	(26, 34)	(27, 34)	(27, 9)
(35, 15)	(35, 15)	(38, 28)	(33, 9)	(13, 28)	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)	(35, 28)	(26, 34)	(27, 34)	(27, 9)	(26, 9)
(38, 28)	(38, 28)	(33, 9)	(13, 28)	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)	(35, 28)	(26, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)
(33, 9)	(33, 9)	(13, 28)	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)	(35, 28)	(26, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)	(38, 28)
(13, 28)	(13, 28)	$\mathcal{O}$	(13, 15)	(33, 34)	(38, 15)	(35, 28)	(26, 34)	(27, 34)	(27, 9)	(26, 9)	(35, 15)	(38, 28)	(33, 9)

Now that we have constructed a “large” cyclic prime-order subgroup of  $BLS6\_6$  suitable for many pen-and-paper computations in elliptic curve cryptography, we have to look at how to do pairings in this context. We know that  $BLS6\_6$  is a pairing-friendly curve by design, since it has a small embedding degree  $k = 6$ . It is therefore possible to compute Weil pairings efficiently. However, in order to do so, we have to decide the groups  $\mathbb{G}_1$  and  $\mathbb{G}_2$  as explained in exercise 76.

check  
reference

Since  $BLS6\_6$  has two non-trivial subgroups, it would be possible to use any of them as the  $n$ -torsion group. However, in cryptography, the only secure choice is to use the large prime-order subgroup, which in our case is  $BLS6\_6[13]$ . We therefore decide to consider the 13-torsion and define  $G_1[13]$  as the first argument for the Weil pairing function:

$$\mathbb{G}_1[13] = \{(13, 15) \rightarrow (33, 34) \rightarrow (38, 15) \rightarrow (35, 28) \rightarrow (26, 34) \rightarrow (27, 34) \rightarrow (27, 9) \rightarrow (26, 9) \rightarrow (35, 15) \rightarrow (38, 28) \rightarrow (33, 9) \rightarrow (13, 28) \rightarrow \mathcal{O}\}$$

In order to construct the domain for the second argument, we need to construct  $\mathbb{G}_2[13]$ , which, according to the general theory, should be defined by those elements  $P$  of the full 13-torsion group  $BLS6\_6[13]$  that are mapped to  $43 \cdot P$  under the Frobenius endomorphism (equation 5.24).

check  
reference

To compute  $\mathbb{G}_2[13]$ , we therefore have to find the full 13-torsion group first. To do so, we use the technique from XXX, which tells us that the full 13-torsion can be found in the curve extension over the extension field  $\mathbb{F}_{43^6}$ , since the embedding degree of  $BLS6\_6$  is 6:

$$BLS6\_6 := \{(x, y) \mid y^2 = x^3 + 6 \text{ for all } x, y \in \mathbb{F}_{43^6}\} \quad (5.42)$$

Thus, we have to construct  $\mathbb{F}_{43^6}$ , a field that contains 6321363049 elements. In order to do so, we use the procedure of XXX and start by choosing a non-reducible polynomial of degree 6 from the ring of polynomials  $\mathbb{F}_{43}[t]$ . We choose  $p(t) = t^6 + 6$ . Using Sage, we get the following:

add refer-  
ence

```
sage: F43 = GF(43) 623
sage: F43t.<t> = F43[] 624
sage: p = F43t(t^6+6) 625
sage: p.is_irreducible() 626
True 627
sage: F43_6.<v> = GF(43^6, name='v', modulus=p) 628
```

Recall from XXX that elements  $x \in \mathbb{F}_{43^6}$  can be seen as polynomials  $a_0 + a_1v + a_2v^2 + \dots + a_5v^5$  with the usual addition of polynomials and multiplication modulo  $t^6 + 6$ .

add refer-  
ence

In order to compute  $\mathbb{G}_2[13]$ , we first have to extend  $BLS6\_6$  to  $\mathbb{F}_{43^6}$ , that is, we keep the defining equation, but expand the domain from  $\mathbb{F}_{43}$  to  $\mathbb{F}_{43^6}$ . After that, we have to find at least one element  $P$  from that curve that is not the point at infinity, is in the full 13-torsion and satisfies the identity  $\pi(P) = [43]P$ . We can then use this element as our generator of  $\mathbb{G}_2[13]$  and construct all other elements by repeatedly adding the generator to itself.

Since  $BLS6(\mathbb{F}_{43^6})$  contains 6321251664 elements, it's not a good strategy to simply loop through all elements. Fortunately, Sage has a way to loop through elements from the torsion group directly:

```
sage: BLS6 = EllipticCurve(F43_6, [0, 6]) # curve extension 629
sage: INF = BLS6(0) # point at infinity 630
```

```

4110 sage: for P in INF.division_points(13): # full 13-torsion          631
4111 .....: # PI(P) == [q]P                                           632
4112 .....:         if P.order() == 13: # exclude point at infinity    633
4113 .....:             PiP = BLS6([a.frobenius() for a in P])          634
4114 .....:             qP = 43*P                                         635
4115 .....:             if PiP == qP:                                     636
4116 .....:                 break                                         637
4117 sage: P.xy()                                                         638
4118 (7*v^2, 16*v^3)                                                     639

```

4119 We found an element from the full 13-torsion that is in the Eigenspace of the Eigenvalue 43,  
4120 which implies that it is an element of  $\mathbb{G}_2[13]$ . As  $\mathbb{G}_2[13]$  is cyclic of prime order, this element  
4121 must be a generator:

$$g_{\mathbb{G}_2[13]} = (7v^2, 16v^3) \quad (5.43)$$

4122 We can use this generator to compute  $\mathbb{G}_2$  in logarithmic order with respect to  $g_{\mathbb{G}_2[13]}$ . Using  
4123 Sage we get the following:

```

4124 sage: Q = BLS6(7*v^2, 16*v^3)                                       640
4125 sage: BLS6_13_2 = []                                               641
4126 sage: for x in range(0, 13):                                       642
4127 .....:     P = x*Q                                                 643
4128 .....:     BLS6_13_2.append(P)                                     644

```

$$\begin{aligned} \mathbb{G}_2 = \{ & (7v^2, 16v^3) \rightarrow (10v^2, 28v^3) \rightarrow (42v^2, 16v^3) \rightarrow (37v^2, 27v^3) \rightarrow \\ & (16v^2, 28v^3) \rightarrow (17v^2, 28v^3) \rightarrow (17v^2, 15v^3) \rightarrow (16v^2, 15v^3) \rightarrow \\ & (37v^2, 16v^3) \rightarrow (42v^2, 27v^3) \rightarrow (10v^2, 15v^3) \rightarrow (7v^2, 27v^3) \rightarrow \mathcal{O} \} \end{aligned}$$

Again, having a logarithmic description of  $\mathbb{G}_2[13]$  is tremendously helpful in pen-and-paper computations, as it reduces complicated computation in the extended curves to modular 13 arithmetics, as in the following example:

$$\begin{aligned} (17v^2, 28v^3) \oplus (10v^2, 15v^3) &= [6](7v^2, 16v^3) \oplus [11](7v^2, 16v^3) \\ &= [6 + 11](7v^2, 16v^3) \\ &= [4](7v^2, 16v^3) \\ &= (37v^2, 27v^3) \end{aligned}$$

4129 So XXX is really all we need to do computations in  $\mathbb{G}_2[13]$  in this book efficiently.

4130 To summarize the previous steps, we have found two subgroups,  $\mathbb{G}_1[13]$  and  $\mathbb{G}_2[13]$  suit-  
4131 able to do Weil pairings on  $BLS6\_6$  as explained in 5.28. Using the logarithmic order XXX  
4132 of  $\mathbb{G}_1[13]$ , the logarithmic order XXX of  $\mathbb{G}_2[13]$  and the bilinearity in 5.44, we can do Weil  
4133 pairings on  $BLS6\_6$  in a pen-and-paper style:

$$e([k_1]g_{BLS6\_6[13]}, [k_2]g_{\mathbb{G}_2[13]}) = e(g_{BLS6\_6[13]}, g_{\mathbb{G}_2[13]})^{k_1 \cdot k_2} \quad (5.44)$$

4134 Observe that the Weil pairing between our two generators is given by the following identity:

$$e(g_{BLS6\_6[13]}, g_{\mathbb{G}_2[13]}) = 5v^5 + 16v^4 + 16v^3 + 15v^2 + 3v + 41 \quad (5.45)$$

add refer-  
ence

check  
reference

add refer-  
ence

add refer-  
ence

```

4135 sage: g1 = BLS6([13,15]) 645
4136 sage: g2 = BLS6([7*v^2, 16*v^3]) 646
4137 sage: g1.weil_pairing(g2,13) 647
4138 5*v^5 + 16*v^4 + 16*v^3 + 15*v^2 + 3*v + 41 648

```

4139 **Hashing to pairing groups** We give various constructions to hash into  $\mathbb{G}_1$  and  $\mathbb{G}_2$ .

4140 We start with hashing to the scalar field... **TO APPEAR**

4141 None of these techniques work for hashing into  $\mathbb{G}_2$ . We therefore implement Pederson's

4142 Hash for BLS6.

We start with  $\mathbb{G}_1$ . Our goal is to define an 12-bit bounded hash function:

$$H_1 : \{0,1\}^{12} \rightarrow \mathbb{G}_1$$

Since  $12 = 3 \cdot 4$  we “randomly” select 4 uniformly distributed generators  $\{(38,15), (35,28), (27,34), (38,28)\}$  from  $\mathbb{G}_1$  and use the pseudo-random function from XXX. Therefore, we have to choose a set of 4 randomly generated invertible elements from  $\mathbb{F}_{13}$  for every generator. We choose the following:

$$\begin{aligned}
 (38,15) &: \{2,7,5,9\} \\
 (35,28) &: \{11,4,7,7\} \\
 (27,34) &: \{5,3,7,12\} \\
 (38,28) &: \{6,5,1,8\}
 \end{aligned}$$

4143 Our hash function is then computed as follows:

$$\begin{aligned}
 H_1(x_{11}, x_1, \dots, x_0) = & [2 \cdot 7^{x_{11}} \cdot 5^{x_{10}} \cdot 9^{x_9}](38,15) + [11 \cdot 4^{x_8} \cdot 7^{x_7} \cdot 7^{x_6}](35,28) + \\
 & [5 \cdot 3^{x_5} \cdot 7^{x_4} \cdot 12^{x_3}](27,34) + [6 \cdot 5^{x_2} \cdot 1^{x_1} \cdot 8^{x_0}](38,28)
 \end{aligned}$$

4144 Note that  $a^x = 1$  when  $x = 0$ . Hence, those terms can be omitted in the computation. In  
 4145 particular, the hash of the 12-bit zero string is given as follows:

**WRONG – ORDERING – REDO**

$$\begin{aligned}
 H_1(0) = & [2](38,15) + [11](35,28) + [5](27,34) + [6](38,28) = \\
 & (27,34) + (26,34) + (35,28) + (26,9) = (33,9) + (13,28) = (38,28)
 \end{aligned}$$

The hash of 011010101100 is given as follows:

$$\begin{aligned}
 H_1(011010101100) = & \text{WRONG – ORDERING – REDO} \\
 & [2 \cdot 7^0 \cdot 5^1 \cdot 9^1](38,15) + [11 \cdot 4^0 \cdot 7^1 \cdot 7^0](35,28) + [5 \cdot 3^1 \cdot 7^0 \cdot 12^1](27,34) + [6 \cdot 5^1 \cdot 1^0 \cdot 8^0](38,28) = \\
 & [2 \cdot 5 \cdot 9](38,15) + [11 \cdot 7](35,28) + [5 \cdot 3 \cdot 12](27,34) + [6 \cdot 5](38,28) = \\
 & [12](38,15) + [12](35,28) + [11](27,34) + [4](38,28) =
 \end{aligned}$$

**TO APPEAR**

We can use the same technique to define a 12-bit bounded hash function in  $\mathbb{G}_2$ :

$$H_2 : \{0,1\}^{12} \rightarrow \mathbb{G}_2$$

finish  
writing  
this up

add refer-  
ence

correct  
computa-  
tions

fill in  
missing  
parts

Again, we “randomly” select 4 uniformly distributed generators  $\{(7v^2, 16v^3), (42v^2, 16v^3), (17v^2, 15v^3), (10v^2, 15v^3)\}$  from  $\mathbb{G}_2$ , and use the pseudo-random function from XXX. Therefore, we have to choose a set of 4 randomly generated invertible elements from  $\mathbb{F}_{13}$  for every generator:

add reference

$$\begin{aligned} (7v^2, 16v^3) &: \{8, 4, 5, 7\} \\ (42v^2, 16v^3) &: \{12, 1, 3, 8\} \\ (17v^2, 15v^3) &: \{2, 3, 9, 11\} \\ (10v^2, 15v^3) &: \{3, 6, 9, 10\} \end{aligned}$$

Our hash function is then computed like this:

$$H_1(x_{11}, x_{10}, \dots, x_0) = [8 \cdot 4^{x_{11}} \cdot 5^{x_{10}} \cdot 7^{x_9}](7v^2, 16v^3) + [12 \cdot 1^{x_8} \cdot 3^{x_7} \cdot 8^{x_6}](42v^2, 16v^3) + [2 \cdot 3^{x_5} \cdot 9^{x_4} \cdot 11^{x_3}](17v^2, 15v^3) + [3 \cdot 6^{x_2} \cdot 9^{x_1} \cdot 10^{x_0}](10v^2, 15v^3)$$

We extend this to a hash function that maps unbounded bitstrings to  $\mathbb{G}_2$  by precomposing with an actual hash function like MD5, and feed the first 12 bits of its outcome into our previously defined hash function, with  $TinyMD5_{\mathbb{G}_2}(s) = H_2(MD5(s)_{11}, \dots, MD5(s)_0)$ :

$$TinyMD5_{\mathbb{G}_2} : \{0, 1\}^* \rightarrow \mathbb{G}_2$$

For example, since  $MD5(“”) =$

$0xd41d8cd98f00b204e9800998ecf8427e$ , and the binary representation of the hexadecimal number  $0x27e$  is  $001001111110$ , we compute  $TinyMD5_{\mathbb{G}_2}$  of the empty string as follows:

$$TinyMD5_{\mathbb{G}_2}(“”) = H_2(MD5(s)_{11}, \dots, MD5(s)_0) = H_2(001001111110) =$$

check equation

# Chapter 6

## Statements

As we have seen in the informal introduction XXX, a SNARK is a short non-interactive argument of knowledge, where the knowledge-proof attests to the correctness of statements like “The prover knows the prime factorization of a given number” or “The prover knows the preimage to a given SHA2 digest value” and similar things. However, human-readable statements like these are imprecise and not very useful from a formal perspective.

In this chapter we therefore look more closely at ways to formalize statements in mathematically rigorous ways, useful for SNARK development. We start by introducing formal languages as a way to define statements properly (section 6.1). We will then look at algebraic circuits and rank-1 constraint systems as two particularly useful ways to define statements in certain formal languages (section 6.2). After that, we will have a look at fundamental building blocks of compilers that compile high-level languages to circuits and associated rank-1 constraint systems.

Proper statement design should be of high priority in the development of SNARKs, since unintended true statements can lead to potentially severe and almost undetectable security vulnerabilities in the applications of SNARKs.

### 6.1 Formal Languages

Formal languages provide the theoretical background in which statements can be formulated in a logically rigorous way and where proving the correctness of any given statement can be realized by computing words in that language.

One might argue that the understanding of formal languages is not very important in SNARK development and associated statement design, but terms from that field of research are standard jargon in many papers on zero-knowledge proofs. We therefore believe that at least some introduction to formal languages and how they fit into the picture of SNARK development is beneficial, mostly to give developers a better intuition about where all this is located in the bigger picture of the logic landscape. In addition, formal languages give a better understanding of what a formal proof for a statement actually is.

Roughly speaking, a formal language (or just language for short) is nothing but a set of words, *th*. Words, in turn, are strings of letters taken from some alphabet and formed according to some defining rules of the language.

To be more precise, let  $\Sigma$  be any set and  $\Sigma^*$  the set of all finite **tuples** (ordered lists)  $(x_1, \dots, x_n)$  of elements  $x_j$  from  $\Sigma$  including the empty tuple  $() \in \Sigma^*$ . Then, a **language**  $L$ , in its most general definition, is nothing but a subset of  $\Sigma^*$ . In this context, the set  $\Sigma$  is called the **alphabet** of the language  $L$ , elements from  $\Sigma$  are called letters and elements from  $L$  are called **words**. The rules that specify which tuples from  $\Sigma^*$  belong to the language and which don't,

Chapter  
1?

"rigorous"?

"proving"?



are called the **grammar** of the language. S: I suggest adding an example based on English, e.g. “tea” and “eat” are words of English, but “aet” and “tae” are not

Add ex-ample

If  $L_1$  and  $L_2$  are two formal languages over the same alphabet, we call  $L_1$  and  $L_2$  **equivalent** if they generate the same set of words.

M: 1:1 correspondence might actually be wrong

**Decision Functions** Our previous definition of formal languages is very general and many subclasses of languages are known in the literature. However, in the context of SNARK development, languages are commonly defined as **decision problems** where a so-called **deciding relation**  $R \subset \Sigma^*$  decides whether a given tuple  $x \in \Sigma^*$  is a word in the language or not. If  $x \in R$  then  $x$  is a word in the associated language  $L_R$  and if  $x \notin R$  then not. The relation  $R$  therefore summarizes the grammar of language  $L_R$ .

Unfortunately, in some literature on proof systems,  $x \in R$  is often written as  $R(x)$ , which is misleading since in general  $R$  is not a function but a relation in  $\Sigma^*$ . For the sake of this book, we therefore adopt a different point of view and work with what we might call a **decision function** instead:

$$R : \Sigma^* \rightarrow \{true, false\} \quad (6.1)$$

Decision functions decide if a tuple  $x \in \Sigma^*$  is an element of a language or not. In case a decision function is given, the associated language itself can be written as the set of all tuples that are decided by  $R$ , i.e as the set:

$$L_R := \{x \in \Sigma^* \mid R(x) = true\} \quad (6.2)$$

In the context of formal languages and decision problems, a **statement**  $S$  is the claim that language  $L$  contains a word  $x$ , i.e a statement claims that there exist some  $x \in L$ . A constructive **proof** for statement  $S$  is given by some string  $P \in \Sigma^*$  and such a proof is **verified** by checking  $R(P) = true$ . In this case,  $P$  is called an **instance** of the statement  $S$ .

While the term **language** might suggest a deeper relation to the well known **natural languages** like English, formal languages and natural languages differ in many ways. The following examples will provide some intuition about formal languages, highlighting the concepts of statements, proofs and instances:

*Example 106 (Alternating Binary strings).* To consider a very basic formal language with an almost trivial grammar, consider the set  $\{0, 1\}$  of the two letters 0 and 1 as our alphabet  $\Sigma$  and imply the rule that a proper word must consist of alternating binary letters of arbitrary length.

Then, the associated language  $L_{alt}$  is the set of all finite binary tuples, where a 1 must follow a 0 and vice versa. So, for example,  $(1, 0, 1, 0, 1, 0, 1, 0, 1) \in L_{alt}$  is a proper word in this languages as is  $(0) \in L_{alt}$  or the empty word  $() \in L_{alt}$ . However, the binary tuple  $(1, 0, 1, 0, 1, 0, 1, 1, 1) \in \{0, 1\}^*$  is not a proper word, as it violates the grammar of  $L_{alt}$ : the last3 letters are all 1. Furthermore, the tuple  $(0, A, 0, A, 0, A, 0)$  is not a proper word, as not all its letters are not from the proper alphabet: we defined the alphabet  $\Sigma$  as the set  $\{0, 1\}$ , and  $A$  is not part of that set.

Attempting to write the grammar of this language in a more formal way, we can define the following decision function:

$$R : \{0, 1\}^* \rightarrow \{true, false\} ; (x_0, x_1, \dots, x_n) \mapsto \begin{cases} true & x_{j-1} \neq x_j \text{ for all } 1 \leq j \leq n \\ false & \text{else} \end{cases}$$

We can use this function to decide if arbitrary **binary tuples** are words in  $L_{alt}$  or not. Some examples are given below:

binary tuples

- $R(1, 0, 1) = true$ ,



- 4220 •  $R(0) = \text{true}$ ,
- 4221 •  $R() = \text{true}$ ,
- 4222 • but  $R(1, 1) = \text{false}$ .

4223 Inside our language  $L_{alt}$ , it makes sense to claim the following statement: “There exists an  
 4224 alternating string.” One way to prove this statement constructively is by providing an actual  
 4225 instance, that is, finding actual alternating string like  $x = (1, 0, 1)$ . Constructing string  $(1, 0, 1)$   
 4226 therefore proves the statement “There exists an alternating string.”, because it is easy to verify  
 4227 that  $R(1, 0, 1) = \text{true}$ .

4228 *Example 107 (Programming Language).* Programming languages are a very important class of  
 4229 formal languages. For these languages, the alphabet is usually (a subset) of the ASCII table,  
 4230 and the grammar is defined by the rules of the programming language’s compiler. Words, then,  
 4231 are nothing but properly written computer programs that the compiler accepts. The compiler  
 4232 can therefore be interpreted as the decision function.

4233 To give an unusual example strange enough to highlight the point, consider the program-  
 4234 ming language Malbolge as defined in XXX. This language was specifically designed to be  
 4235 almost impossible to use and writing programs in this language is a difficult task. An inter-  
 4236 esting claim is therefore the statement: “There exists a computer program in Malbolge”. As it  
 4237 turned out, proving this statement constructively, that is, by providing an actual instance of such  
 4238 a program, was not an easy task, as it took two years after the introduction of Malbolge to write  
 4239 a program that its compiler accepts. So, for two years, no one was able to prove the statement  
 4240 constructively.

To look at this high-level description more formally, we write  $L_{Malbolge}$  for the language that  
 uses the ASCII table as its alphabet and its words are tuples of ASCII letters that the Malbolge  
 compiler accepts. Proving the statement “There exists a computer program in Malbolge” is then  
 equivalent to the task of finding some word  $x \in L_{Malbolge}$ . The string

(=<#9] 6ZY327Uv4-QsqpMn&+Ij''E%e{Ab w=\_:]Kw%o44Uqp0/Q?xNvL:'H%c#DD2^WV>gY;dts76qKJImZkj

4241 is an example of such a proof, as it is excepted by the Malbolge compiler and is compiled to  
 4242 an executable binary that displays “Hello, World.” (See XXX). In this example, the Malbolge  
 4243 compiler therefore serves as the verification process.

4244 *Example 108 (The Empty Language).* To see that not every language has even one word, con-  
 4245 sider the alphabet  $\Sigma = \mathbb{Z}_6$ , where  $\mathbb{Z}_6$  is the ring of modular 6 arithmetics as derived in example  
 4246 9 in chapter ??, together with the following decision function

$$R_0 : \mathbb{Z}_6^* \rightarrow \{\text{true}, \text{false}\} ; (x_1, \dots, x_n) \mapsto \begin{cases} \text{true} & n = 4 \text{ and } x_1 \cdot x_1 = 2 \\ \text{false} & \text{else} \end{cases}$$

4244 We write  $L_0$  for the associated language. As we can see from the multiplication table of  $\mathbb{Z}_6$  in  
 4245 example 9 in chapter ??, the ring  $\mathbb{Z}_6$  does not contain any element  $x$  such that  $x^2 = 2$ , which  
 4246 implies  $R_0(x_1, \dots, x_n) = \text{false}$  for all tuples  $(x_1, \dots, x_n) \in \Sigma^*$ . The language therefore does  
 4247 not contain any words. Proving the statement “There exists a word in  $L_0$ ” constructively by  
 4248 providing an instance is therefore impossible. The verification will never check any tuple.

4249 *Example 109 (3-Factorization).* We will use the following simple example repeatedly through-  
 4250 out this book. The task is to develop a SNARK that proves knowledge of three factors of an  
 4251 element from the finite field  $\mathbb{F}_{13}$ . There is nothing particularly useful about this example from

add refer-  
ence

add refer-  
ence

check  
reference

check  
reference

an application point of view, however, in a sense, it is the most simple example that gives rise to a non trivial SNARK in some of the most common zero-knowledge proof systems.

Formalizing the high-level description, we use  $\Sigma := \mathbb{F}_{13}$  as the underlying alphabet of this problem and define the language  $L_{3.fac}$  to consists of those tuples of field elements from  $\mathbb{F}_{13}$  that contain exactly 4 letters  $w_1, w_2, w_3, w_4$  which satisfy the equation  $w_1 \cdot w_2 \cdot w_3 = w_4$ .

So, for example, the tuple  $(2, 12, 4, 5)$  is a word in  $L_{3.fac}$ , while neither  $(2, 12, 11)$ , nor  $(2, 12, 4, 7)$  nor  $(2, 12, 7, 168)$  are words in  $L_{3.fac}$  as they don't satisfy the grammar or are not define over the proper alphabet.

We can describe the language  $L_{3.fac}$  more formally by introducing a decision function (as described in equation 6.1):

$$R_{3.fac} : \mathbb{F}_{13}^* \rightarrow \{true, false\} ; (x_1, \dots, x_n) \mapsto \begin{cases} true & n = 4 \text{ and } x_1 \cdot x_2 \cdot x_3 = x_4 \\ false & \text{else} \end{cases}$$

Having defined the language  $L_{3.fac}$ , it then makes sense to claim the statement “There is a word in  $L_{3.fac}$ ”. The way  $L_{3.fac}$  is designed, this statement is equivalent to the statement “There are four elements  $w_1, w_2, w_3, w_4$  from the finite field  $\mathbb{F}_{13}$  such that the equation  $w_1 \cdot w_2 \cdot w_3 = w_4$  holds.”

Proving the correctness of this statement constructively means to actually find some concrete field elements like  $x_1 = 2, x_2 = 12, x_3 = 4$  and  $x_4 = 5$  that satisfy the relation  $R_{3.fac}$ . The tuple  $(2, 12, 4, 5)$  is therefore a constructive proof for the statement and the computation  $R_{3.fac}(2, 12, 4, 5) = true$  is a verification of that proof. In contrast, the tuple  $(2, 12, 4, 7)$  is not a proof of the statement, since the check  $R_{3.fac}(2, 12, 4, 7) = false$  does not verify the proof.

**Example 110 (Tiny-jubjub Membership).** In one of our main examples, we derive a SNARK that proves a pair  $(x, y)$  of field elements from  $\mathbb{F}_{13}$  to be a point on the tiny-jubjub curve in its Edwards form (see section 5.1.3).

In the first step, we define a language such that points on the tiny-jubjub curve are in 1:1 correspondence with words in that language.

Since the tiny-jubjub curve is an elliptic curve over the field  $\mathbb{F}_{13}$ , we choose the alphabet  $\Sigma = \mathbb{F}_{13}$ . In this case, the set  $\mathbb{F}_{13}^*$  consists of all finite strings of field elements from  $\mathbb{F}_{13}$ . To define the grammar, recall from 69 that a point on the tiny-jubjub curve is a pair  $(x, y)$  of field elements such that  $3 \cdot x^2 + y^2 = 1 + 8 \cdot x^2 \cdot y^2$ . We can use this equation to derive the following decision function:

$$R_{tiny.jj} : \mathbb{F}_{13}^* \rightarrow \{true, false\} ; (x_1, \dots, x_n) \mapsto \begin{cases} true & n = 2 \text{ and } 3 \cdot x_1^2 + x_2^2 = 1 + 8 \cdot x_1^2 \cdot x_2^2 \\ false & \text{else} \end{cases}$$

The associated language  $L_{tiny.jj}$  is then given as the set of all strings from  $\mathbb{F}_{13}^*$  that are mapped onto *true* by  $R_{tiny.jj}$ . We get

$$L_{tiny.jj} = \{(x_1, \dots, x_n) \in \mathbb{F}_{13}^* \mid R_{tiny.jj}(x_1, \dots, x_n) = true\}$$

We can claim the statement “There is a word in  $L_{tiny.jj}$ ” and because  $L_{tiny.jj}$  is defined by  $R_{tiny.jj}$ , this statement is equivalent to the claim “The tiny-jubjub curve in its Edwards form has curve a point.”

A constructive proof for this statement is a pair  $(x, y)$  of field elements that satisfies the Edwards equation. Example 69 therefore implies that the tuple  $(11, 6)$  is a constructive proof and the computation  $R_{tiny.jj}(11, 6) = true$  is a proof verification. In contrast, the tuple  $(1, 1)$  is not a proof of the statement, since the check  $R_{tiny.jj}(1, 1) = false$  does not verify the proof.

Are we using  $w$  and  $x$  interchangeably or is there a difference between them?

check reference

jubjub

check reference

check reference

check wording

check reference

*Exercise 51.* Consider exercise XXX again. Define a decision function such that the associated language  $L_{Exercise_{XXX}}$  consist precisely of all solutions to the equation  $5x + 4 = 28 + 2x$  over  $\mathbb{F}_{13}$ . Provide a constructive proof for the claim: “There exist a word in  $L_{Exercise_{XXX}}$  and verify the proof.

*Exercise 52.* Consider the modular 6 arithmetics  $\mathbb{Z}_6$  from example 9 in chapter ??, the alphabet  $\Sigma = \mathbb{Z}_6$  and the decision function

$$R_{example\_9} : \Sigma^* \rightarrow \{true, false\} ; x \mapsto \begin{cases} true & x.len() = 1 \text{ and } 3 \cdot x + 3 = 0 \\ false & \text{else} \end{cases}$$

Compute all words in the associated language  $L_{example\_9}$ , provide a constructive proof for the statement “There exist a word in  $L_{example\_example\_9}$ ” and verify the proof.

check  
references

**Instance and Witness** As we have seen in the previous paragraph, statements provide membership claims in formal languages, and instances serve as constructive proofs for those claims. However, in the context of **zero-knowledge** proof systems, our naive notion of constructive proofs is refined in such a way that its possible to hide parts of the proof instance and still be able to prove the statement. In this context, it is therefore necessary to split a proof into a **public part** called the **instance** and a private part called a **witness**.

To account for this separation of a proof instance into a public and a private part, our previous definition of formal languages needs a refinement in the context of zero-knowledge proof systems. Instead of a single alphabet, the refined definition considers two alphabets  $\Sigma_I$  and  $\Sigma_W$ , and a decision function defined as follows:

$$R : \Sigma_I^* \times \Sigma_W^* \rightarrow \{true, false\} ; (i; w) \mapsto R(i; w) \quad (6.3)$$

Words are therefore tuples  $(i; w) \in \Sigma_I^* \times \Sigma_W^*$  with  $R(i; w) = true$ . The refined definition differentiates between public inputs  $i \in \Sigma_I$  and private inputs  $w \in \Sigma_W$ . The public input  $i$  is called an **instance** and the private input  $w$  is called a **witness** of  $R$ .

If a decision function is given, the associated language is defined as the set of all tuples from the underlying alphabet that are verified by the decision function:

$$L_R := \{(i; w) \in \Sigma_I^* \times \Sigma_W^* \mid R(i; w) = true\} \quad (6.4)$$

In this refined context, a **statement**  $S$  is a claim that, given an instance  $i \in \Sigma_I^*$ , there is a witness  $w \in \Sigma_W^*$  such that language  $L$  contains a word  $(i; w)$ . A constructive **proof** for statement  $S$  is given by some string  $P = (i; w) \in \Sigma_I^* \times \Sigma_W^*$  and a proof is **verified** by checking  $R(P) = true$ .

It is worth understanding the difference between statements as defined in XXX and the refined notion of statements from this paragraph. While statements in the sense of the previous paragraph can be seen as membership claims, statements in the refined definition can be seen as knowledge-proofs, where a prover claims knowledge of a witness for a given instance. For a more detailed discussion on this topic see [XXX sec 1.4]

add refer-  
ence

add refer-  
ence

*Example 111 (SHA256 – Knowledge of Preimage).* One of the most common examples in the context of zero-knowledge proof systems is the **knowledge-of-a-preimage proof** for some cryptographic hash function like *SHA256*, where a publicly known *SHA256* digest value is given, and the task is to prove knowledge of a preimage for that digest under the *SHA256* function, without revealing that preimage.

To understand this problem in detail, we have to introduce a language able to describe the knowledge-of-preimage problem in such a way that the claim “Given digest  $i$ , there is a

preimage  $w$  such that  $SHA256(w) = i$ ” becomes a statement in that language. Since  $SHA256$  is a function

$$SHA256 : \{0, 1\}^* \rightarrow \{0, 1\}^{256}$$

that maps binary strings of arbitrary length onto binary strings of length 256 and we want to prove knowledge of preimages, we have to consider binary strings of size 256 as instances and binary strings of arbitrary length as witnesses.

An appropriate alphabet  $\Sigma_I$  for the set of all instances and an appropriate alphabet  $\Sigma_W$  for the set of all witnesses is therefore given by the set  $\{0, 1\}$  of the two binary letters and a proper decision function is given by:

$$R_{SHA256} : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{true, false\};$$

$$(i; w) \mapsto \begin{cases} true & i.len() = 256, i = SHA256(w) \\ false & else \end{cases}$$

We write  $L_{SHA256}$  for the associated language and note that it consists of words, which are tuples  $(i; w)$  such that the instance  $i$  is the  $SHA256$  image of the witness  $w$ .

Given some instance  $i \in \{0, 1\}^{256}$ , a statement in  $L_{SHA256}$  is the claim “Given digest  $i$ , there is a preimage  $w$  such that  $SHA256(w) = i$ ”, which is exactly what the knowledge-of-preimage problem is about. A constructive proof for this statement is therefore given by a preimage  $w$  to the digest  $i$  and proof verification is achieved by checking that  $SHA256(w) = i$ .

*Example 112 (3-factorization).* To give an intuition about the implication of refined languages, consider  $L_{3, fac}$  from example 109 again. As we have seen, a constructive proof in  $L_{3, fac}$  is given by 4 field elements  $x_1, x_2, x_3$  and  $x_4$  from  $\mathbb{F}_{13}$  such that the product in modular 13 arithmetics of the first three elements is equal to the 4'th element.

Splitting words from  $L_{3, fac}$  into private and public parts, we can reformulate the problem and introduce different levels of privacy into the problem. For example, we could reformulate the membership statement of  $L_{3, fac}$  into a statement where all factors  $x_1, x_2, x_3$  of  $x_4$  are private and only the product  $x_4$  is public. A statement for this reformulation is then expressed by the claim: “Given a publicly known field element  $x_4$ , there are three private factors of  $x_4$ ”. Assuming some instance  $x_4$ , a constructive proof for the associated knowledge claim is then provided by any tuple  $(x_1, x_2, x_3)$  such that  $x_1 \cdot x_2 \cdot x_3 = x_4$ .

At this point, it is important to note that, while constructive proofs in the refinement don't look very different from constructive proofs in the original language, we will see in XXX that there are proof systems able to prove the statement (at least with high probability) without revealing anything about the factors  $x_1, x_2$ , or  $x_3$ . This is why the importance of the refinement only becomes clear once more elaborate proofing methods beyond naive constructive proofs are provided.

We can formalize this new language, which we might call  $L_{3, fac\_zk}$ , by defining the following decision function:

*Definition 6.1.0.1.*

$$R_{3, fac\_zk} : \mathbb{F}_{13}^* \times \mathbb{F}_{13}^* \rightarrow \{true, false\};$$

$$((i_1, \dots, i_n); (w_1, \dots, w_m)) \mapsto \begin{cases} true & n = 1, m = 3, i_1 = w_1 \cdot w_2 \cdot w_3 \\ false & else \end{cases}$$

The associated language  $L_{3, fac\_zk}$  is defined by all tuples from  $\mathbb{F}_{13}^* \times \mathbb{F}_{13}^*$  that are mapped onto *true* under the decision function  $R_{3, fac\_zk}$ .

check  
reference

add refer-  
ence

Considering the distinction we made between the instance and the witness part in  $L_{3, fac\_zk}$ , one might ask why we chose the factors  $x_1, x_2$  and  $x_3$  to be the witness and the product  $x_4$  to be the instance and why we didn't choose another combination? This was an arbitrary choice in the example. Every other combination of private and public factors would be equally valid. For example, it would be possible to declare all variables as private or to declare all variables as public. Actual choices are determined by the application only.

*Example 113 (The Tiny-Jubjub Curve).* Consider the language  $L_{tiny.jj}$  from example 110. As we have seen, a constructive proof in  $L_{tiny.jj}$  is given by a pair  $(x_1, x_2)$  of field elements from  $\mathbb{F}_{13}$  such that the pair is a point of the tiny-jubjub curve in its Edwards representation.

check  
reference

We look at a reasonable splitting of words from  $L_{tiny.jj}$  into private and public parts. The two obvious choices are to either choose both coordinates  $x_1$  as  $x_2$  as public inputs, or to choose both coordinates  $x_1$  as  $x_2$  as private inputs.

In case both coordinates are public, we define the grammar of the associated language by introducing the following decision function:

$$R_{tiny.jj.1} : \mathbb{F}_{13}^* \times \mathbb{F}_{13}^* \rightarrow \{true, false\} ;$$

$$(I_1, \dots, I_n; W_1, \dots, W_m) \mapsto \begin{cases} true & n = 2, m = 0 \text{ and } 3 \cdot I_1^2 + I_2^2 = 1 + 8 \cdot I_1^2 \cdot I_2^2 \\ false & else \end{cases}$$

The language  $L_{tiny.jj.1}$  is defined as the set of all strings from  $\mathbb{F}_{13}^* \times \mathbb{F}_{13}^*$  that are mapped onto *true* by  $R_{tiny.jj.1}$ .

In case both coordinates are private, we define the grammar of the associated refined language by introducing the following decision function:

$$R_{tiny.jj.zk} : \mathbb{F}_{13}^* \times \mathbb{F}_{13}^* \rightarrow \{true, false\} ;$$

$$(I_1, \dots, I_n; W_1, \dots, W_m) \mapsto \begin{cases} true & n = 0, m = m \text{ and } 3 \cdot W_1^2 + W_2^2 = 1 + 8 \cdot W_1^2 \cdot W_2^2 \\ false & else \end{cases}$$

The language  $L_{tiny.jj.zk}$  is defined as the set of all strings from  $\mathbb{F}_{13}^* \times \mathbb{F}_{13}^*$  that are mapped onto *true* by  $R_{tiny.jj.zk}$ .

*Exercise 53.* Consider the modular 6 arithmetics  $\mathbb{Z}_6$  from example 9 in chapter ?? as alphabets  $\Sigma_I$  and  $\Sigma_W$  and the following decision function

check  
reference

$$R_{linear} : \Sigma^* \times \Sigma^* \rightarrow \{true, false\} ;$$

$$(i; w) \mapsto \begin{cases} true & i.len() = 3 \text{ and } w.len() = 1 \text{ and } i_1 \cdot w_1 + i_2 = i_3 \\ false & else \end{cases}$$

Which of the following instances  $(i_1, i_2, i_3)$  has a proof of knowledge in  $L_{linear}$ ?

• (3, 3, 0)

• (2, 1, 0)

• (4, 4, 2)

*Exercise 54 (Edwards Addition on Tiny-Jubjub).* Consider the tiny-jubjub curve together with its Edwards addition law from example XXX. Define an instance alphabet  $\Sigma_I$ , a witness alphabet  $\Sigma_W$  and a decision function  $R_{add}$  with associated language  $L_{add}$  such that a string  $(i; w) \in \Sigma_I^* \times$

add refer-  
ence



4369  $\Sigma_W^*$  is a word in  $L_{add}$  if and only if  $i$  is a pair of curve points on the tiny-jubjub curve in Edwards  
 4370 form and  $w$  is the Edwards sum of those curve points.

4371 Choose some instance  $i \in \Sigma_I^*$ , provide a constructive proof for the statement “There is a  
 4372 witness  $w \in \Sigma_W^*$  such that  $(i;w)$  is a word in  $L_{add}$ ” and verify that proof. Then find some  
 4373 instance  $i \in \Sigma_I^*$  such that  $i$  has no knowledge proof in  $L_{add}$ .

4374 **Modularity** From a developers perspective, it is often useful to construct complex statements  
 4375 and their representing languages from simple ones. In the context of zero-knowledge proof  
 4376 systems, those simple building blocks are often called **gadgets**, and gadget libraries usually  
 4377 contain representations of atomic types like booleans, integers, various hash functions, elliptic  
 4378 curve cryptography and many more. In order to synthesize statements, developers then combine  
 4379 predefined gadgets into complex logic. We call the ability to combine statements into more  
 4380 complex statements **modularity**.

4381 To understand the concept of modularity on the level of formal languages defined by deci-  
 4382 sion functions, we need to look at the **intersection** of two languages, which exists whenever  
 4383 both languages are defined over the same alphabet. In this case, the intersection is a language  
 4384 that consists of strings which are words in both languages.

4385 To be more precise, let  $L_1$  and  $L_2$  be two languages defined over the same instance and  
 4386 witness alphabets  $\Sigma_I$  and  $\Sigma_W$ . Then the intersection  $L_1 \cap L_2$  of  $L_1$  and  $L_2$  is defined as

$$L_1 \cap L_2 := \{x \mid x \in L_1 \text{ and } x \in L_2\} \quad (6.5)$$

4387 If both languages are defined by decision functions  $R_1$  and  $R_2$ , the following function is a  
 4388 decision function for the intersection language  $L_1 \cap L_2$ :

$$R_{L_1 \cap L_2} : \Sigma_I^* \times \Sigma_W^* \rightarrow \{true, false\}; (i, w) \mapsto R_1(i, w) \text{ and } R_2(i, w) \quad (6.6)$$

4389 Thus, the intersection of two decision-function-based languages is a also decision-function-  
 4390 based language. This is important from an implementations point of view: It allows us to  
 4391 construct complex decision functions, their languages and associated statements from simple  
 4392 building blocks. Given a publicly known instance  $i \in \Sigma_I^*$  a statement in an intersection language  
 4393 then claims knowledge of a witness that satisfies all relations simultaneously.

## 4394 6.2 Statement Representations

4395 As we have seen in the previous section, formal languages and their definitions by decision  
 4396 functions are a powerful tool to describe statements in a formally rigorous manner.

4397 However, from the perspective of existing zero-knowledge proof systems, not all ways to  
 4398 actually represent decision functions are equally useful. Depending on the proof system, some  
 4399 are more suitable than others. In this section, will describe two of the most common ways to  
 4400 represent decision functions and their statements.

### 4401 6.2.1 Rank-1 Quadratic Constraint Systems

4402 Although decision functions are expressible in various ways, many contemporary proofing sys-  
 4403 tems require the deciding relation to be expressed in terms of a system of quadratic equations  
 4404 over a finite field. This is true in particular for pairing-based proofing systems like XXX,  
 4405 roughly because it is possible to check solutions to those equations “in the exponent” of pairing-  
 4406 friendly cryptographic groups.

add refer-  
ence

In this section, we will therefore have a closer look at a particular type of quadratic equation called **rank-1 quadratic constraints systems**, which are a common standard in zero-knowledge proof systems. We will start with a general introduction to those systems and then look at their relation to formal languages. We will look into a common way to compute solutions to those systems, and then show how a simple compiler might derive rank-1 constraint systems from more high-level programming code.

**R1CS representation** To understand what **rank-1 (quadratic) constraint systems** are in detail, let  $\mathbb{F}$  be a field,  $n, m$  and  $k \in \mathbb{N}$  three numbers and  $a_j^i, b_j^i$  and  $c_j^i \in \mathbb{F}$  constants from  $\mathbb{F}$  for every index  $0 \leq j \leq n+m$  and  $1 \leq i \leq k$ . Then a rank-1 constraint system (R1CS) is defined as follows:

*Definition 6.2.1.1. R1CS representation*

$$\begin{aligned} (a_0^1 + \sum_{j=1}^n a_j^1 \cdot I_j + \sum_{j=1}^m a_{n+j}^1 \cdot W_j) \cdot (b_0^1 + \sum_{j=1}^n b_j^1 \cdot I_j + \sum_{j=1}^m b_{n+j}^1 \cdot W_j) &= c_0^1 + \sum_{j=1}^n c_j^1 \cdot I_j + \sum_{j=1}^m c_{n+j}^1 \cdot W_j \\ &\vdots \\ (a_0^k + \sum_{j=1}^n a_j^k \cdot I_j + \sum_{j=1}^m a_{n+j}^k \cdot W_j) \cdot (b_0^k + \sum_{j=1}^n b_j^k \cdot I_j + \sum_{j=1}^m b_{n+j}^k \cdot W_j) &= c_0^k + \sum_{j=1}^n c_j^k \cdot I_j + \sum_{j=1}^m c_{n+j}^k \cdot W_j \end{aligned}$$

If a rank-1 constraint system is given, the parameter  $k$  is called the **number of constraints**. If a tuple  $(I_1, \dots, I_n; W_1, \dots, W_m)$  of field elements satisfies these equations,  $(I_1, \dots, I_n)$  is called an **instance** and  $(W_1, \dots, W_m)$  is called an associated **witness** of the system.

*Remark 3 (Matrix notation).* The presentation of rank-1 constraint systems can be simplified using the notation of vectors and matrices, which abstracts over the indices. In fact if  $x = (1, I, W) \in \mathbb{F}^{1+n+m}$  is a  $(n+m+1)$ -dimensional vector,  $A, B, C$  are  $(n+m+1) \times k$ -dimensional matrices and  $\odot$  is the **Schur/Hadamard product**, then a R1CS can be written as

$$Ax \odot Bx = Cx$$

However, since we did not introduced matrix calculus in the book, we use XXX as the defining equation for rank-1 constraints systems. We only highlighted the matrix notation, because it is sometimes used in the literature.

Generally speaking, the idea of a rank-1 constraint system is to keep track of all the values that any variable can assume during a computation and to bind the relationships among all those variables that are implied by the computation itself. Enforcing relations between all the steps of a computer program, the execution is then constrained to be computed in exactly the expected way without any opportunity for deviations. In this sense, solutions to rank-1 constraint systems are proofs of proper program execution.

*Example 114 (3-Factorization).* To provide a better intuition of rank-1 constraint systems, consider the language  $L_{3, \text{fac\_zk}}$  from example 109 again. As we have seen,  $L_{3, \text{fac\_zk}}$  consists of words  $(I_1; W_1, W_2, W_3)$  over the alphabet  $\mathbb{F}_{13}$  such that  $I_1 = W_1 \cdot W_2 \cdot W_3$ . We show how to rewrite the decision function as a rank-1 constraint system.

Since R1CS are systems of quadratic equations, expressions like  $W_1 \cdot W_2 \cdot W_3$  which contain products of more than two factors (which are therefore not quadratic) have to be rewritten in a process often called **flattening**. To flatten the defining equation  $I_1 = W_1 \cdot W_2 \cdot W_3$  of  $L_{3, \text{fac\_zk}}$  we introduce a new variable  $W_4$ , which captures two of the three multiplications in  $W_1 \cdot W_2 \cdot W_3$ . We get the following two constraints

$$\begin{aligned} W_1 \cdot W_2 &= W_4 && \text{constraint 1} \\ W_4 \cdot W_3 &= I_1 && \text{constraint 2} \end{aligned}$$

Given some instance  $I_1$ , any solution  $(W_1, W_2, W_3, W_4)$  to this system of equations provides a solution to the original equation  $I_1 = W_1 \cdot W_2 \cdot W_3$  and vice versa. Both equations are therefore equivalent in the sense that solutions are in a 1:1 correspondence.

Looking at both equations, we see how each constraint enforces a step in the computation. In fact, the first constraint forces any computation to multiply the witness  $W_1$  and  $W_2$  first. Otherwise it would not be possible to compute the witness  $W_4$ , which is needed to solve the second constraint. Witness  $W_4$  therefore expresses the constraining of an intermediate computational state.

At this point, one might ask why equation 1 constrains the system to compute  $W_1 \cdot W_2$  first, since computing  $W_2 \cdot W_3$ , or  $W_1 \cdot W_3$  in the beginning and then multiplying with the remaining factor gives the exact same result. The reason is that the way we designed the R1CS prohibits any of these alternative computations, which shows that R1CS are in general **not unique** descriptions of a language: many different R1CS are able to describe the same problem.

To see that the two quadratic equations qualify as a rank-1 constraint system, choose the parameter  $n = 1, m = 4$  and  $k = 2$  as well as

$$\begin{array}{llllll} a_0^1 = 0 & a_1^1 = 0 & a_2^1 = 1 & a_3^1 = 0 & a_4^1 = 0 & a_5^1 = 0 \\ a_0^2 = 0 & a_1^2 = 0 & a_2^2 = 0 & a_3^2 = 0 & a_4^2 = 0 & a_5^2 = 1 \\ \\ b_0^1 = 0 & b_1^1 = 0 & b_2^1 = 0 & b_3^1 = 1 & b_4^1 = 0 & b_5^1 = 0 \\ b_0^2 = 0 & b_1^2 = 0 & b_2^2 = 0 & b_3^2 = 0 & b_4^2 = 1 & b_5^2 = 0 \\ \\ c_0^1 = 0 & c_1^1 = 0 & c_2^1 = 0 & c_3^1 = 0 & c_4^1 = 0 & c_5^1 = 1 \\ c_0^2 = 0 & c_1^2 = 1 & c_2^2 = 0 & c_3^2 = 0 & c_4^2 = 0 & c_5^2 = 0 \end{array}$$

With this choice, the rank-1 constraint system of our 3-factorization problem can be written in its most general form as follows:

$$\begin{aligned} (a_0^1 + a_1^1 I_1 + a_2^1 W_1 + a_3^1 W_2 + a_4^1 W_3 + a_5^1 W_4) \cdot (b_0^1 + b_1^1 I_1 + b_2^1 W_1 + b_3^1 W_2 + b_4^1 W_3 + b_5^1 W_4) &= (c_0^1 + c_1^1 I_1 + c_2^1 W_1 + c_3^1 W_2 + c_4^1 W_3 + c_5^1 W_4) \\ (a_0^2 + a_1^2 I_1 + a_2^2 W_2 + a_3^2 W_2 + a_4^2 W_3 + a_5^2 W_4) \cdot (b_0^2 + b_1^2 I_1 + b_2^2 W_2 + b_3^2 W_2 + b_4^2 W_3 + b_5^2 W_4) &= (c_0^2 + c_1^2 I_1 + c_2^2 W_2 + c_3^2 W_2 + c_4^2 W_3 + c_5^2 W_4) \end{aligned}$$

*Example 115* (The Tiny-Jubjub curve). Consider the languages  $L_{\text{tiny.jj.1}}$  from example 110, which consist of words  $(I_1, I_2)$  over the alphabet  $\mathbb{F}_{13}$  such that  $3 \cdot I_1^2 + I_2^2 = 1 + 8 \cdot I_1^2 \cdot I_2^2$ .

We derive a rank-1 constraint system such that its associated language is equivalent to  $L_{\text{tiny.jj.1}}$ . To achieve this, we first rewrite the defining equation:

$$\begin{aligned} 3 \cdot I_1^2 + I_2^2 &= 1 + 8 \cdot I_1^2 \cdot I_2^2 && \Leftrightarrow \\ 0 &= 1 + 8 \cdot I_1^2 \cdot I_2^2 - 3 \cdot I_1^2 - I_2^2 && \Leftrightarrow \\ 0 &= 1 + 8 \cdot I_1^2 \cdot I_2^2 + 10 \cdot I_1^2 + 12 \cdot I_2^2 \end{aligned}$$

Since R1CSs are systems of quadratic equations, we have to reformulate this expression into a system of quadratic equations. To do so, we have to introduce new variables that constrain intermediate steps in the computation and we have to decide if those variables should be public or private. We decide to declare all new variables as private and get the following constraints

$$\begin{array}{ll} I_1 \cdot I_1 = W_1 & \text{constraint 1} \\ I_2 \cdot I_2 = W_2 & \text{constraint 2} \\ (8 \cdot W_1) \cdot W_2 = W_3 & \text{constraint 3} \\ (12 \cdot W_2 + W_3 + 10 \cdot W_1 + 1) \cdot 1 = 0 & \text{constraint 4} \end{array}$$

check  
reference



To see that these four quadratic equations qualify as a rank-1 constraint system according to definition XXX, choose the parameter  $n = 2$ ,  $m = 3$  and  $k = 4$ :

add reference

$$\begin{array}{llllll} a_0^1 = 0 & a_1^1 = 1 & a_2^1 = 0 & a_3^1 = 0 & a_4^1 = 0 & a_5^1 = 0 \\ a_0^2 = 0 & a_1^2 = 0 & a_2^2 = 1 & a_3^2 = 0 & a_4^2 = 0 & a_5^2 = 0 \\ a_0^3 = 0 & a_1^3 = 0 & a_2^3 = 0 & a_3^3 = 8 & a_4^3 = 0 & a_5^3 = 0 \\ a_0^4 = 1 & a_1^4 = 0 & a_2^4 = 0 & a_3^4 = 10 & a_4^4 = 12 & a_5^4 = 1 \end{array}$$

$$\begin{array}{llllll} b_0^1 = 0 & b_1^1 = 1 & b_2^1 = 0 & b_3^1 = 0 & b_4^1 = 0 & b_5^1 = 0 \\ b_0^2 = 0 & b_1^2 = 0 & b_2^2 = 1 & b_3^2 = 0 & b_4^2 = 0 & b_5^2 = 0 \\ b_0^3 = 0 & b_1^3 = 0 & b_2^3 = 0 & b_3^3 = 0 & b_4^3 = 1 & b_5^3 = 0 \\ b_0^4 = 1 & b_1^4 = 0 & b_2^4 = 0 & b_3^4 = 0 & b_4^4 = 0 & b_5^4 = 0 \end{array}$$

$$\begin{array}{llllll} c_0^1 = 0 & c_1^1 = 0 & c_2^1 = 0 & c_3^1 = 1 & c_4^1 = 0 & c_5^1 = 0 \\ c_0^2 = 0 & c_1^2 = 0 & c_2^2 = 0 & c_3^2 = 0 & c_4^2 = 1 & c_5^2 = 0 \\ c_0^3 = 0 & c_1^3 = 0 & c_2^3 = 0 & c_3^3 = 0 & c_4^3 = 0 & c_5^3 = 1 \\ c_0^4 = 0 & c_1^4 = 0 & c_2^4 = 0 & c_3^4 = 0 & c_4^4 = 0 & c_5^4 = 0 \end{array}$$

With this choice, the rank-1 constraint system of our tiny-jubjub curve point problem can be written in its most general form as follows:

$$\begin{aligned} (a_0^1 + a_1^1 I_1 + a_2^1 I_2 + a_3^1 W_1 + a_4^1 W_2 + a_5^1 W_3) \cdot (b_0^1 + b_1^1 I_1 + b_2^1 I_2 + b_3^1 W_1 + b_4^1 W_2 + b_5^1 W_3) &= (c_0^1 + c_1^1 I_1 + c_2^1 I_2 + c_3^1 W_1 + c_4^1 W_2 + c_5^1 W_3) \\ (a_0^2 + a_1^2 I_1 + a_2^2 I_2 + a_3^2 W_1 + a_4^2 W_2 + a_5^2 W_3) \cdot (b_0^2 + b_1^2 I_1 + b_2^2 I_2 + b_3^2 W_1 + b_4^2 W_2 + b_5^2 W_3) &= (c_0^2 + c_1^2 I_1 + c_2^2 I_2 + c_3^2 W_1 + c_4^2 W_2 + c_5^2 W_3) \\ (a_0^3 + a_1^3 I_1 + a_2^3 I_2 + a_3^3 W_1 + a_4^3 W_2 + a_5^3 W_3) \cdot (b_0^3 + b_1^3 I_1 + b_2^3 I_2 + b_3^3 W_1 + b_4^3 W_2 + b_5^3 W_3) &= (c_0^3 + c_1^3 I_1 + c_2^3 I_2 + c_3^3 W_1 + c_4^3 W_2 + c_5^3 W_3) \\ (a_0^4 + a_1^4 I_1 + a_2^4 I_2 + a_3^4 W_1 + a_4^4 W_2 + a_5^4 W_3) \cdot (b_0^4 + b_1^4 I_1 + b_2^4 I_2 + b_3^4 W_1 + b_4^4 W_2 + b_5^4 W_3) &= (c_0^4 + c_1^4 I_1 + c_2^4 I_2 + c_3^4 W_1 + c_4^4 W_2 + c_5^4 W_3) \end{aligned}$$

4448 In what follows, we write  $L_{jubjub}$  for the associated language that consists of solutions to the  
4449 R1CS.

4450 To see that  $L_{jubjub}$  is equivalent to  $L_{tiny.jj.1}$ , let  $(I_1, I_2; W_1, W_2, W_3)$  be a word in  $L_{jubjub}$ , then  
4451  $(I_1, I_2)$  is a word in  $L_{tiny.jj.1}$ , since the defining R1CS of  $L_{jubjub}$  implies that  $I_1$  and  $I_2$  satisfy the  
4452 Edwards equation of the tiny-jubjub curve. On the other hand, let  $(I_1, I_2)$  be a word in  $L_{tiny.jj.1}$ .  
4453 Then  $(I_1, I_2; I_1^2, I_2^2, 8 \cdot I_1^2 \cdot I_2^2)$  is a word in  $L_{jubjub}$  and both maps are inverses of each other.

4454 **Exercise 55.** Consider the language  $L_{tiny.jj\_zk}$  and define a rank-1 constraint relation with a  
4455 decision function such that the associated language is equivalent to  $L_{tiny.jj\_zk}$ .

4456 **R1CS Satisfiability** To understand how rank-1 constraint systems define formal languages,  
4457 observe that every R1CS over a field  $\mathbb{F}$  defines a decision function over the alphabet  $\Sigma_I \times \Sigma_W =$   
4458  $\mathbb{F} \times \mathbb{F}$  in the following way:

$$R_{R1CS} : \mathbb{F}^* \times \mathbb{F}^* \rightarrow \{true, false\} ; (I; W) \mapsto \begin{cases} true & (I; W) \text{ satisfies R1CS} \\ false & \text{else} \end{cases} \quad (6.7)$$

4459 Every R1CS therefore defines a formal language. The grammar of this language is encoded  
4460 in the constraints, words are solutions to the equations and a **statement** is a knowledge claim  
4461 “Given instance  $I$ , there is a witness  $W$  such that  $(I; W)$  is a solution to the rank-1 constraint  
4462 system”. A constructive proof to this claim is therefore an assignment of a field element to every  
4463 witness variable, which is verified whenever the set of all instance and witness variables solves  
4464 the R1CS.

*Remark 4 (R1CS satisfiability).* It should be noted that in our definition, every R1CS defines its own language. However, in more theoretical approaches, another language usually called **R1CS satisfiability** is often considered, which is useful when it comes to more abstract problems like expressiveness or the computational complexity of the class of **all** R1CS. From our perspective, the R1CS satisfiability language is obtained by the union of all R1CS languages that are in our definition. To be more precise, let the alphabet  $\Sigma = \mathbb{F}$  be a field. Then

$$L_{R1CS\_SAT}(\mathbb{F}) = \{(i; w) \in \Sigma^* \times \Sigma^* \mid \text{there is a R1CS } R \text{ such that } R(i; w) = \text{true}\}$$

4465 *Example 116 (3-Factorization).* Consider the language  $L_{3.fac\_zk}$  from example 109 and the  
 4466 R1CS defined in example ex:3-factorization-r1cs. As we have seen in ex:3-factorization-r1cs,  
 4467 solutions to the R1CS are in 1:1 correspondence with solutions to the decision function of  
 4468  $L_{3.fac\_zk}$ . Both languages are therefore equivalent in the sense that there is a 1:1 correspon-  
 4469 dence between words in both languages.

check  
referencecheck  
referencecheck  
reference

To give an intuition of what constructive proofs in  $L_{3.fac\_zk}$  look like, consider the instance  $I_1 = 11$ . To prove the statement “There exists a witness  $W$  such that  $(I_1; W)$  is a word in  $L_{3.fac\_zk}$ ” constructively, a proof has to provide assignments to all witness variables  $W_1, W_2, W_3$  and  $W_4$ . Since the alphabet is  $\mathbb{F}_{13}$ , an example assignment is given by  $W = (2, 3, 4, 6)$  since  $(I_1; W)$  satisfies the R1CS

$$\begin{array}{ll} W_1 \cdot W_2 = W_4 & \# 2 \cdot 3 = 6 \\ W_4 \cdot W_3 = I_1 & \# 6 \cdot 4 = 11 \end{array}$$

4470 A proper constructive proof is therefore given by  $P = (2, 3, 4, 6)$ . Of course,  $P$  is not the only  
 4471 possible proof for this statement. Since factorization is not unique in a field in general, another  
 4472 constructive proof is given by  $P' = (3, 5, 12, 2)$ .

*Example 117 (The tiny-jubjub curve).* Consider the language  $L_{jubjub}$  from example 110 and  
 its associated R1CS. To see how constructive proofs in  $L_{jubjub}$  look like, consider the instance  
 $(I_1, I_2) = (11, 6)$ . To prove the statement “There exists a witness  $W$  such that  $(I_1, I_2; W)$  is a  
 word in  $L_{jubjub}$ ” constructively, a proof has to provide assignments to all witness variables  $W_1,$   
 $W_2$  and  $W_3$ . Since the alphabet is  $\mathbb{F}_{13}$ , an example assignment is given by  $W = (4, 10, 8)$  since  
 $(I_1, I_2; W)$  satisfies the R1CS

check  
reference

$$\begin{array}{ll} I_1 \cdot I_1 = W_1 & 11 \cdot 11 = 4 \\ I_2 \cdot I_2 = W_2 & 6 \cdot 6 = 10 \\ (8 \cdot W_1) \cdot W_2 = W_3 & (8 \cdot 4) \cdot 10 = 8 \\ (12 \cdot W_2 + W_3 + 10 \cdot W_1 + 1) \cdot 1 = 0 & 12 \cdot 10 + 8 + 10 \cdot 4 + 1 = 0 \end{array}$$

4473 A proper constructive proof is therefore given by  $P = (4, 10, 8)$ , which shows that the instance  
 4474  $(11, 6)$  is a point on the tiny-jubjub curve.

4475 **Modularity** As we discussed on page 138 XXX, it is often useful to construct complex state-  
 4476 ments and their representing languages from simple ones. Rank-1 constraint systems are par-  
 4477 ticularly useful for this, as the intersection of two R1CS over the same alphabet results in a new  
 4478 R1CS over that same alphabet.

check  
reference

4479 To be more precise, let  $S_1$  and  $S_2$  be two R1CS over  $\mathbb{F}$ , then a new R1CS  $S_3$  is obtained  
 4480 by the intersection  $S_3 = S_1 \cap S_2$  of  $S_1$  and  $S_2$ . In this context, intersection means that both the  
 4481 equations of  $S_1$  **and** the equations of  $S_2$  have to be satisfied in order to provide a solution for the  
 4482 system  $S_3$ .

As a consequence, developers are able to construct complex R1CS from simple ones and this modularity provides the theoretical foundation for many R1CS compilers, as we will see in XXX.

add reference

## 6.2.2 Algebraic Circuits

As we have seen in the previous paragraphs, rank-1 constraint systems are quadratic equations such that solutions are knowledge proofs for the existence of words in associated languages. From the perspective of a proofer, it is therefore important to solve those equations efficiently.

However, in contrast to systems of linear equation, no general methods are known that solve systems of quadratic equations efficiently. Rank-1 constraint systems are therefore impractical from a proofers perspective and auxiliary information is needed that helps to compute solutions efficiently.

Methods which compute R1CS solutions are sometimes called **witness generator functions**. To provide a common example, we introduce another class of decision functions called **algebraic circuits**. As we will see, every algebraic circuit defines an associated R1CS and also provides an efficient way to compute solutions for that R1CS.

It can be shown that every space- and time-bounded computation is expressible as an algebraic circuit. Transforming high-level computer programs into those circuits is a process often called **flattening**.

To understand this in more detail, we will introduce our model for algebraic circuits and look at the concept of circuit execution and valid assignments. After that, we will show how to derive rank-1 constraint systems from circuits and how circuits are useful to compute solutions to their R1CS efficiently.

**Algebraic circuit representation** To see what algebraic circuits are, let  $\mathbb{F}$  be a field. An algebraic circuit is then a directed acyclic (multi)graph that computes a polynomial function over  $\mathbb{F}$ . Nodes with only outgoing edges (source nodes) represent the variables and constants of the function and nodes with only incoming edges (sink nodes) represent the outcome of the function. All other nodes have exactly two incoming edges and represent the defining field operations **addition** as well as **multiplication**. Graph edges represent the flow of the computation along the nodes.

To be more precise, we call a directed acyclic multi-graph  $C(\mathbb{F})$  an **algebraic circuit** over  $\mathbb{F}$  in this book if the following conditions hold:

*Definition 6.2.2.1. Algebraic circuit*

- The set of edges has a total order.
- Every source node has a label that represents either a variable or a constant from the field  $\mathbb{F}$ .
- Every sink node has exactly one incoming edge and a label that represents either a variable or a constant from the field  $\mathbb{F}$ .
- Every node that is neither a source nor a sink has exactly two incoming edges and a label from the set  $\{+, *\}$  that represents either addition or multiplication in  $\mathbb{F}$ .
- All outgoing edges from a node have the same label.
- Outgoing edges from a node with a label that represents a variable have a label.

- Outgoing edges from a node with a label that represents multiplication have a label, if there is at least one labeled edge in both input path.
- All incoming edges to sink nodes have a label.
- If an edge has two labels  $S_i$  and  $S_j$  it gets a new label  $S_i = S_j$ .
- No other edge has a label.
- Incoming edges to sink nodes that are labeled with a constant  $c \in \mathbb{F}$  are labeled with the same constant. Every other edge label is taken from the set  $\{W, I\}$  and indexed compatible with the order of the edge set.

It should be noted that the details in the definitions of algebraic circuits vary between different sources. We use this definition as it is conceptually straightforward and well-suited for pen-and-paper computations.

To get a better intuition of our definition, let  $C(\mathbb{F})$  be an algebraic circuit. Source nodes are the inputs to the circuit and either represent variables or constants. In a similar way, sink nodes represent termination points of the circuit and are either output variables or constants. Constant sink nodes enforce computational outputs to take on certain values.

Nodes that are neither source nodes nor sink nodes are called **arithmetic gates**. Arithmetic gates that are decorated with the “+”-label are called **addition-gates** and arithmetic gates that are decorated with the “·”-label are called **multiplication-gates**. Every arithmetic gate has exactly two inputs, represented by the two incoming edges.

Since the set of edges is ordered, we can write it as  $\{E_1, E_2, \dots, E_n\}$  for some  $n \in \mathbb{N}$  and we use those indices to index the edge labels, too. Edge labels are therefore either constants or symbols like  $I_j$ ,  $W_j$  or  $S_j$ , where  $j$  is an index compatible with the edge order. Labels  $I_j$  represent instance variables, labels  $W_j$  witness variables. Labels on the outgoing edges of input variables constrain the associated variable to that edge. Every other edge defines a constraining equation in the associated R1CS. We will explain this in more detail in XXX.

*Notation and Symbols 12.* In synthesizing algebraic circuits, assigning instance  $I_j$  or witness  $W_j$  labels to appropriate edges is often the final step. It is therefore convenient to not distinguish these two types of edges in previous steps. To account for that, we often simply write  $S_j$  for an edge label, indicating that the private/public property of the label is unspecified and it might represent an instance or a witness label.

*Example 118 (Generalized factorization SNARK).* To give a simple example of an algebraic circuit, consider our 3-factorization problem from example 109 again. To express the problem in the algebraic circuit model, consider the following function

$$f_{3.fac} : \mathbb{F}_{13} \times \mathbb{F}_{13} \times \mathbb{F}_{13} \rightarrow \mathbb{F}_{13}; (x_1, x_2, x_3) \mapsto x_1 \cdot x_2 \cdot x_3$$

Using this function, we can describe the zero-knowledge 3-factorization problem from 109 in the following way: Given instance  $I_1 \in \mathbb{F}_{13}$ , a valid witness is a preimage of  $f_{3.fac}$  at the point  $I_1$ , i.e., a valid witness consists of three values  $W_1$ ,  $W_2$  and  $W_3$  from  $\mathbb{F}_{13}$  such that  $f_{3.fac}(W_1, W_2, W_3) = I_1$ .

To see how this function can be transformed into an algebraic circuit over  $\mathbb{F}_{13}$ , it is a common first step to introduce brackets into the function’s definition and then write the operations as binary operators, in order to highlight how exactly every field operation acts on its two inputs.

add reference

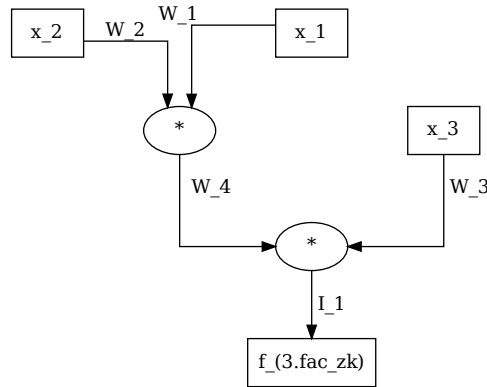
check reference

check reference

Due to the associativity laws in a field, we have several choices. We choose

$$\begin{aligned}
 f_{3.fac}(x_1, x_2, x_3) &= x_1 \cdot x_2 \cdot x_3 && \# \text{ bracket choice} \\
 &= (x_1 \cdot x_2) \cdot x_3 && \# \text{ operator notation} \\
 &= MUL(MUL(x_1, x_2), x_3)
 \end{aligned}$$

4561 Using this expression, we can write an associated algebraic circuit by first constraining the  
 4562 variables to edge labels  $W_1 = x_1$ ,  $W_2 = x_2$  and  $W_3 = x_3$  as well as  $I_1 = f_{3.fac}(x_1, x_2, x_3)$ , taking  
 4563 the distinction between private and public inputs into account. We then rewrite the operator  
 4564 representation of  $f_{3.fac}$  into circuit nodes and get the following:



4565

4566 In this case, the directed acyclic multi-graph is a binary tree with three leaves (the source  
 4567 nodes) labeled by  $x_1$ ,  $x_2$  and  $x_3$ , one root (the single sink node) labeled by  $f(x_1, x_2, x_3)$  and two  
 4568 internal nodes, which are labeled as multiplication gates.

4569 The order we use to label the edges is chosen to make the edge labeling consistent with  
 4570 the choice of  $W_4$  as defined in definition 6.2.2.1. This order can be obtained by a depth-first  
 4571 right-to-left-first traversal algorithm.

check  
reference

*Example 119.* To give a more realistic example of an algebraic circuit, look at the defining  
 equation of the tiny-jubjub curve (69) again. A pair of field elements  $(x, y) \in \mathbb{F}_{13}^2$  is a curve  
 point, precisely if the following equation holds:

check  
reference

$$3 \cdot x^2 + y^2 = 1 + 8 \cdot x^2 \cdot y^2$$

To understand how one might transform this identity into an algebraic circuit, we first rewrite  
 this equation by shifting all terms to the right. We get the following:

$$\begin{aligned}
 3 \cdot x^2 + y^2 &= 1 + 8 \cdot x^2 \cdot y^2 && \Leftrightarrow \\
 0 &= 1 + 8 \cdot x^2 \cdot y^2 - 3 \cdot x^2 - y^2 && \Leftrightarrow \\
 0 &= 1 + 8 \cdot x^2 \cdot y^2 + 10 \cdot x^2 + 12 \cdot y^2
 \end{aligned}$$

Then we use this expression to define a function such that all points of the tiny-jubjub curve are  
 characterized as the function preimages at 0.

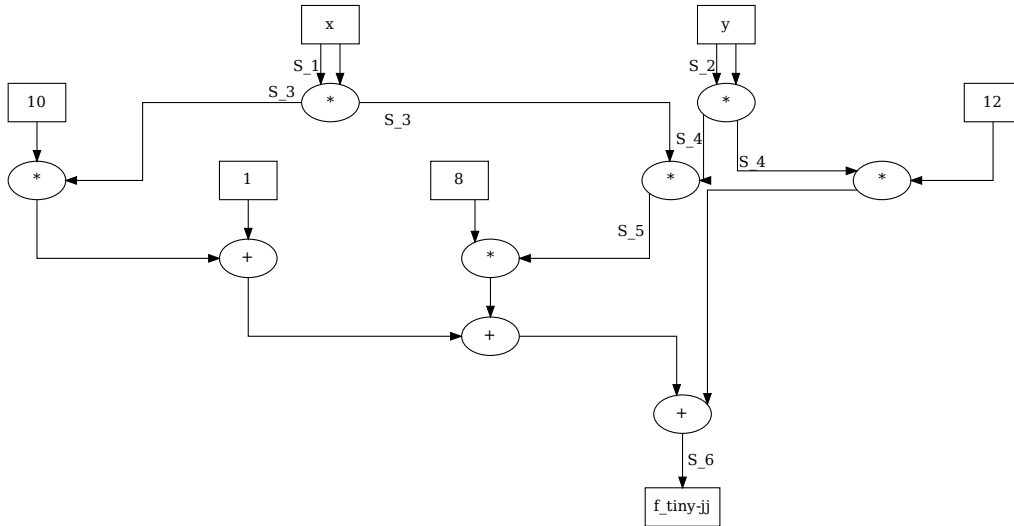
$$f_{tiny-jj} : \mathbb{F}_{13} \times \mathbb{F}_{13} \rightarrow \mathbb{F}_{13} ; (x, y) \mapsto 1 + 8 \cdot x^2 \cdot y^2 + 10 \cdot x^2 + 12 \cdot y^2$$

Every pair of points  $(x, y) \in \mathbb{F}_{13}^2$  with  $f_{\text{tiny-jj}}(x, y) = 0$  is a point on the tiny-jubjub curve, and there are no other curve points. The preimage  $f_{\text{tiny-jj}}^{-1}(0)$  is therefore a complete description of the tiny-jubjub curve.

We can transform this function into an algebraic circuit over  $\mathbb{F}_{13}$ . We first introduce brackets into potentially ambiguous expressions and then rewrite the function in terms of binary operators. We get the following:

$$\begin{aligned}
 f_{\text{tiny-jj}}(x, y) &= 1 + 8 \cdot x^2 \cdot y^2 + 10 \cdot x^2 + 12y^2 && \Leftrightarrow \\
 &= ((8 \cdot ((x \cdot x) \cdot (y \cdot y))) + (1 + 10 \cdot (x \cdot x))) + (12 \cdot (y \cdot y)) && \Leftrightarrow \\
 &= \text{ADD}(\text{ADD}(\text{MUL}(8, \text{MUL}(\text{MUL}(x, x), \text{MUL}(y, y))), \text{ADD}(1, \text{MUL}(10, \text{MUL}(x, x)))), \text{MUL}(12, \text{MUL}(y, y)))
 \end{aligned}$$

Since we haven't decided which part of the computation should be public and which part should be private, we use the unspecified symbol  $S$  to represent edge labels. Constraining all variables to edge labels  $S_1 = x$ ,  $S_2 = y$  and  $S_6 = f_{\text{tiny-jj}}$ , we get the following circuit, representing the function  $f_{\text{tiny-jj}}$ , by inductively replacing binary operators with their associated arithmetic gates:



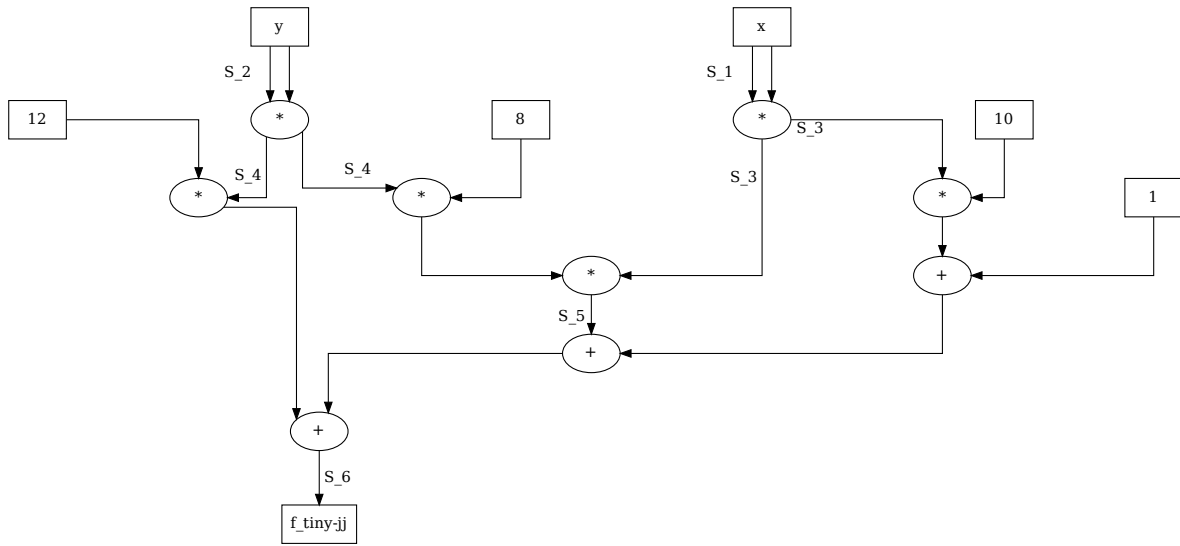
4580

This circuit is not a graph, but a multigraph, since there is more than one edge between some of the nodes.

In the process of designing of circuits from functions, it should be noted that circuit representations are not unique in general. In case of the function  $f_{\text{tiny-jj}}$ , the circuit shape is dependent on our choice of bracketing in XXX. An alternative design i,s for example, given by the following circuit, which occurs when the bracketed expression  $8 \cdot ((x \cdot x) \cdot (y \cdot y))$  is replaced by the expression  $(x \cdot x) \cdot (8 \cdot (y \cdot y))$ .

4588

add reference



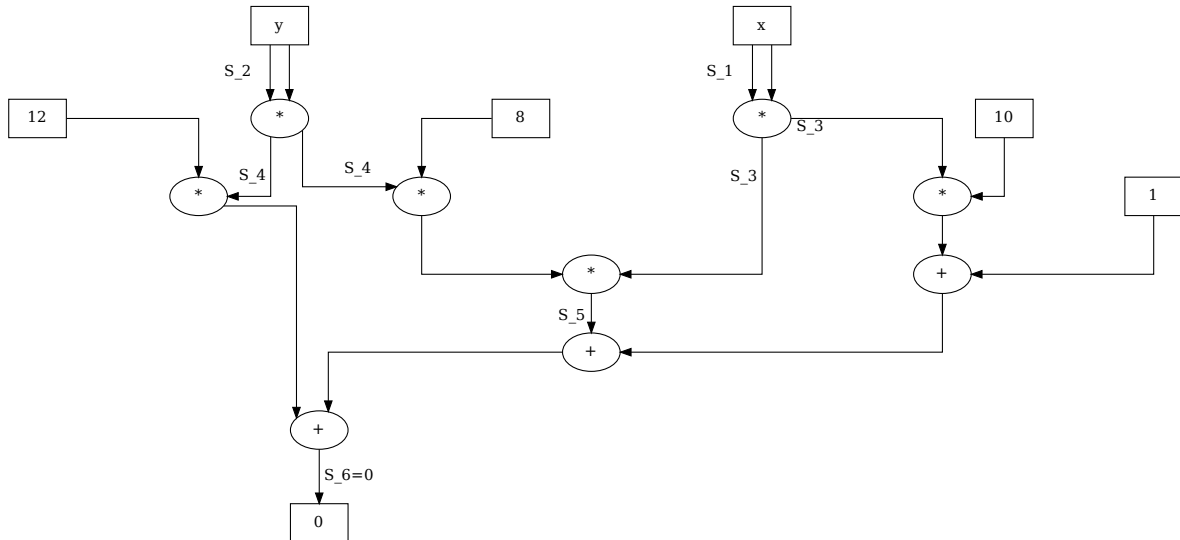
4589

4590

4591 Of course, both circuits represent the same function, due to the associativity and commutativity  
 4592 laws that hold true in any field.

4593 With a circuit that represents the function  $f_{\text{tiny-jj}}$ , we can now proceed to derive a circuit  
 4594 that constrains arbitrary pairs  $(x, y)$  of field elements to be points on the tiny-jubjub curve. To do  
 4595 so, we have to constrain the output to be zero, that is, we have to constrain  $S_6 = 0$ . To indicate  
 4596 this in the circuit, we replace the output variable by the constant 0 and constrain the related edge  
 4597 label accordingly. We get the following:

4598

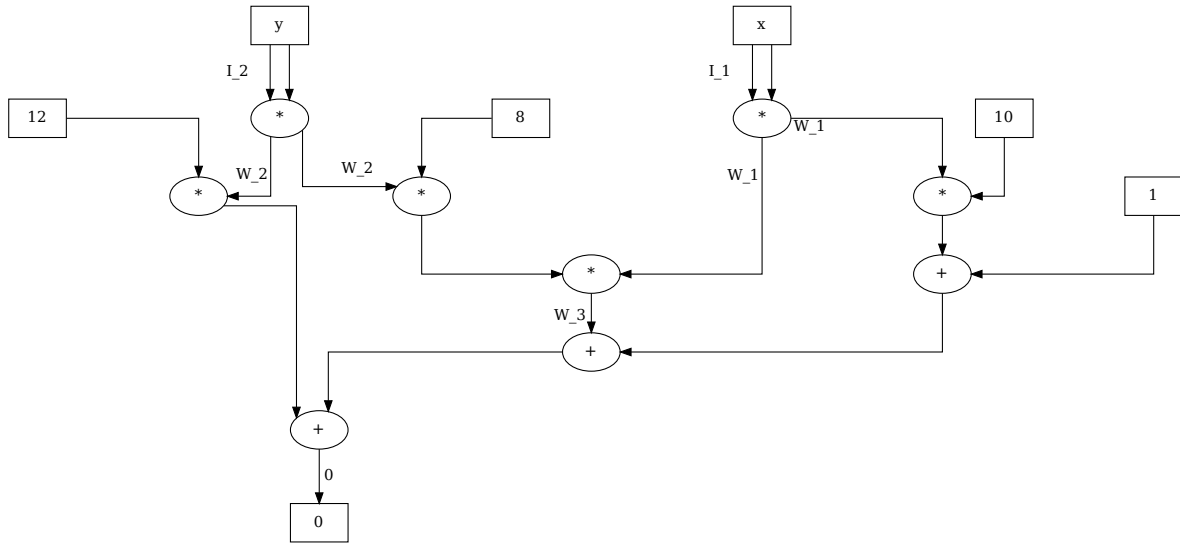


4599

4600

4601 The previous circuit enforces input values assigned to the labels  $S_1$  and  $S_2$  to be points on the  
 4602 tiny-jubjub curve. However, it does not specify which labels are considered public and which  
 4603 are considered private. The following circuit defines the inputs to be public, while all other  
 4604 labels are private:

4605



4606

4607

4608 It can be shown that every space- and time-bounded computation can be transformed into  
 4609 an algebraic circuit. We call any process that transforms a bounded computation into a circuit  
 4610 **flattening**.

4611 **Circuit Execution** Algebraic circuits are directed, acyclic multi-graphs, where nodes repre-  
 4612 sent variables, constants, or addition and multiplication gates. In particular, every algebraic  
 4613 circuit with  $n$  input nodes decorated with variable symbols and  $m$  output nodes decorated with  
 4614 variables can be seen a function that transforms an input tuple  $(x_1, \dots, x_n)$  from  $\mathbb{F}^n$  into an out-  
 4615 put tuple  $(f_1, \dots, f_m)$  from  $\mathbb{F}^m$ . The transformation is done by sending values associated to  
 4616 nodes along their outgoing edges to other nodes. If those nodes are gates, then the values are  
 4617 transformed according to the gate label and the process is repeated along all edges until a sink  
 4618 node is reached. We call this computation **circuit execution**.

4619 When executing a circuit, it is possible to not only compute the output values of the circuit  
 4620 but to derive field elements for all edges, and, in particular, for all edge labels in the circuit. The  
 4621 result is a tuple  $(S_1, S_2, \dots, S_n)$  of field elements associated to all labeled edges, which we call a  
 4622 **valid assignment** to the circuit. In contrast, any assignment  $(S'_1, S'_2, \dots, S'_n)$  of field elements to  
 4623 edge labels that can not arise from circuit execution is called an **invalid assignment**.

4624 Valid assignments can be interpreted as **proofs for proper circuit execution** because they  
 4625 keep a record of the computational result as well as intermediate computational steps.

4626 *Example 120 (3-factorization).* Consider the 3-factorization problem from example 109 and its  
 4627 representation as an algebraic circuit from XXX. We know that the set of edge labels is given  
 4628 by  $S := \{I_1; W_1, W_2, W_3, W_4\}$ .

4629 To understand how this circuit is executed, consider the variables  $x_1 = 2$ ,  $x_2 = 3$  as well as  
 4630  $x_3 = 4$ . Following all edges in the graph, we get the assignments  $W_1 = 2$ ,  $W_2 = 3$  and  $W_3 = 4$ .  
 4631 Then the assignments of  $W_1$  and  $W_2$  enter a multiplication gate and the output of the gate is  
 4632  $2 \cdot 3 = 6$ , which we assign to  $W_4$ , i.e.  $W_4 = 6$ . The values  $W_4$  and  $W_3$  then enter the second  
 4633 multiplication gate and the output of the gate is  $6 \cdot 4 = 11$ , which we assign to  $I_1$ , i.e.  $I_1 = 11$ .

4634 A valid assignment to the 3-factorization circuit  $C_{3, fac}(\mathbb{F}_{13})$  is therefore given by the fol-  
 4635 lowing set:

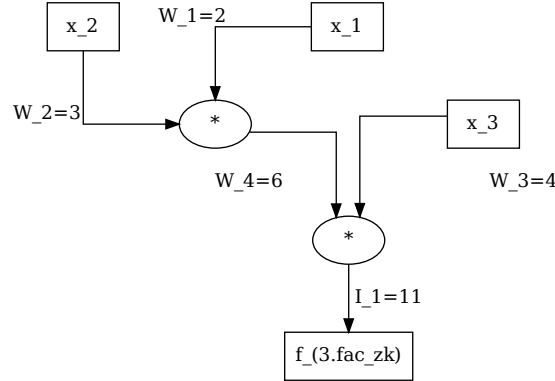
check  
referenceadd refer-  
ence



$$S_{\text{valid}} := \{11; 2, 3, 4, 6\} \quad (6.8)$$

4636

We can visualise this assignment in the circuit as follows:



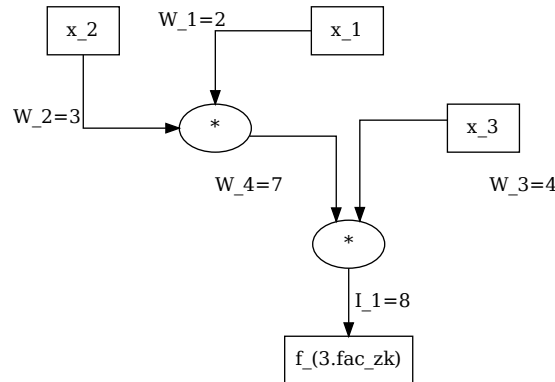
4637

4638

To see what an invalid assignment looks like, consider the assignment  $S_{\text{err}} := \{8; 2, 3, 4, 7\}$ . In

4639

this assignment, the input values are the same as in the previous case. The associated circuit is:



4640

4641

This assignment is invalid, as the assignments of  $I_1$  and  $W_4$  cannot be obtained by executing the circuit.

4642

4643

*Example 121.* To compute a more realistic algebraic circuit execution, consider the defining circuit  $C_{\text{tiny-jj}}(\mathbb{F}_{13})$  from example 117 again. We already know from the way this circuit is constructed that any valid assignment with  $S_1 = x$ ,  $S_2 = y$  and  $S_6 = 0$  will ensure that the pair  $(x, y)$  is a point on the tiny-jubjub curve in its Edwards representation (equation 5.20).

4644

4645

4646

4647

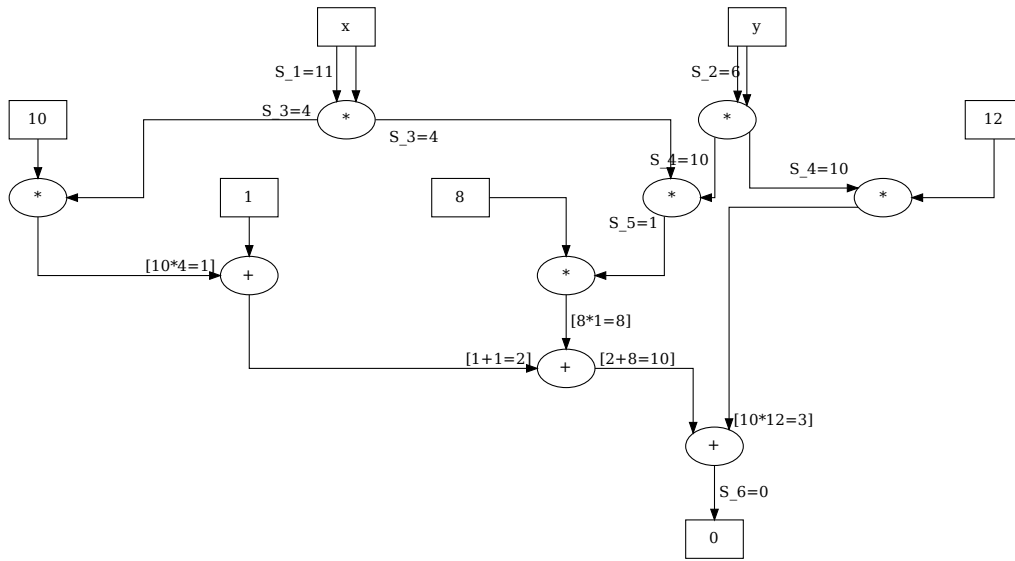
From example 117, we know that the pair  $(11, 6)$  is a proper point on the tiny-jubjub curve and we use this point as input to a circuit execution. We get the following:

4648

check  
reference

check  
reference

check  
reference



4649

Executing the circuit, we indeed compute  $S_6 = 0$  as expected, which proves that  $(11, 6)$  is a point on the tiny-jubjub curve in its Edwards representation. A valid assignment of  $C_{\text{tiny-jj}}(\mathbb{F}_{13})$  is therefore given by the following equation:

$$S_{\text{tiny-jj}} = \{S_1, S_2, S_3, S_4, S_5, S_6\} = \{11, 6, 4, 10, 1, 0\}$$

4650 **Circuit Satisfiability** To understand how algebraic circuits give rise to formal languages, ob-  
 4651 serve that every algebraic circuit  $C(\mathbb{F})$  over a fields  $\mathbb{F}$  defines a decision function over the al-  
 4652 phabet  $\Sigma_I \times \Sigma_W = \mathbb{F} \times \mathbb{F}$  in the following way:

$$R_{C(\mathbb{F})} : \mathbb{F}^* \times \mathbb{F}^* \rightarrow \{true, false\} ; (I; W) \mapsto \begin{cases} true & (I; W) \text{ is valid assignment to } C(\mathbb{F}) \\ false & \text{else} \end{cases} \quad (6.9)$$

4653 Every algebraic circuit therefore defines a formal language. The grammar of this language is  
 4654 encoded in the shape of the circuit, words are assignments to edge labels that are derived from  
 4655 circuit execution, and **statements** are knowledge claims “Given instance  $I$ , there is a witness  
 4656  $W$  such that  $(I; W)$  is a valid assignment to the circuit”. A constructive proof to this claim  
 4657 is therefore an assignment of a field element to every witness variable, which is verified by  
 4658 executing the circuit to see if the assignment of the execution meets the assignment of the  
 4659 proof.

4660 In the context of zero-knowledge proof systems, executing circuits is also often called **wit-**  
 4661 **ness generation**, since in applications the instance part is usually public, while its the task of a  
 4662 prover to compute the witness part.

*Remark 5 (Circuit satisfiability).* It should be noted that, in our definition, every circuit defines its own language. However, in more theoretical approaches another language usually called **circuit satisfiability** is often considered, which is useful when it comes to more abstract problems like expressiveness, or computational complexity of the class of **all** algebraic circuits over a given field. From our perspective the circuit satisfiability language is obtained by union of all circuit languages that are in our definition. To be more precise, let the alphabet  $\Sigma = \mathbb{F}$  be a field. Then

Should we refer to RICS satisfiability (p. 142 here?)

$$L_{\text{CIRCUIT\_SAT}(\mathbb{F})} = \{(i; w) \in \Sigma^* \times \Sigma^* \mid \text{there is a circuit } C(\mathbb{F}) \text{ such that } (i; w) \text{ is valid assignment}\}$$

*Example 122 (3-Factorization).* Consider the circuit  $C_{3, fac}$  from equation 6.8 again. We call the associated language  $L_{3, fac\_circ}$ .

check  
reference

To understand how a constructive proof of a statement in  $L_{3, fac\_circ}$  looks like, consider the instance  $I_1 = 11$ . To provide a proof for the statement “There exist a witness  $W$  such that  $(I_1; W)$  is a word in  $L_{3, fac\_circ}$ ” a proof therefore has to consists of proper values for the variables  $W_1$ ,  $W_2$ ,  $W_3$  and  $W_4$ . Any proofer therefore has to find input values for  $W_1$ ,  $W_2$  and  $W_3$  and then execute the circuit to compute  $W_4$  under the assumption  $I_1 = 11$ .

Example XXX implies that  $(2, 3, 4, 6)$  is a proper constructive proof and in order to verify the proof a verifier needs to execute the circuit with instance  $I_1 = 11$  and inputs  $W_1 = 2$ ,  $W_2 = 3$  and  $W_3 = 4$  to decide whether the proof is a valid assignment or not.

add refer-  
ence

**Associated Constraint Systems** As we have seen in 6.2.1.1, rank-1 constraint systems define a way to represent statements in terms of a system of quadratic equations over finite fields, suitable for pairing-based zero-knowledge proof systems. However, those equations provide no practical way for a proofer to actually compute a solution. On the other hand, algebraic circuits can be executed in order to derive valid assignments efficiently.

check  
reference

In this paragraph, we show how to transform any algebraic circuit into a rank-1 constraint system such that valid circuit assignments are in 1:1 correspondence with solutions to the associated R1CS.

To see this, let  $C(\mathbb{F})$  be an algebraic circuit over a finite field  $\mathbb{F}$ , with a set of edge labels  $\{S_1, S_2, \dots, S_n\}$ . Then one of the following steps is executed for every edge label  $S_j$  from that set:

*Definition 6.2.2.2.* • If the edge label  $S_j$  is an outgoing edge of a multiplication gate, the R1CS gets a new quadratic constraint

$$(\text{left input}) \cdot (\text{right input}) = S_j \quad (6.10)$$

where (left input) respectively (right input) is the output from the symbolic execution of the subgraph that consists of the left respectively right input edge of this gate, and all edges and nodes that have this edge in their path, starting with constant inputs or labeled outgoing edges of other nodes.

- If the edge label  $S_j$  is an outgoing edge of an addition gate, the R1CS gets a new quadratic constraint

$$(\text{left input} + \text{right input}) \cdot 1 = S_j \quad (6.11)$$

where (left input) respectively (right input) is the output from the symbolic execution of the subgraph that consists of the left respectively right input edge of this gate and all edges and nodes that have this edge in their path, starting with constant inputs or labeled outgoing edges of other nodes.

- No other edge label adds a constraint to the system.

The result of this method is a rank-1 constraint system, and, in this sense, every algebraic circuit  $C(\mathbb{F})$  generates a R1CS  $R$ , which we call the **associated R1CS** of the circuit. It can be shown that a tuple of field elements  $(S_1, S_2, \dots, S_n)$  is a valid assignment to a circuit if and only if the same tuple is a solution to the associated R1CS. Circuit executions therefore compute solutions to rank-1 constraints systems efficiently.

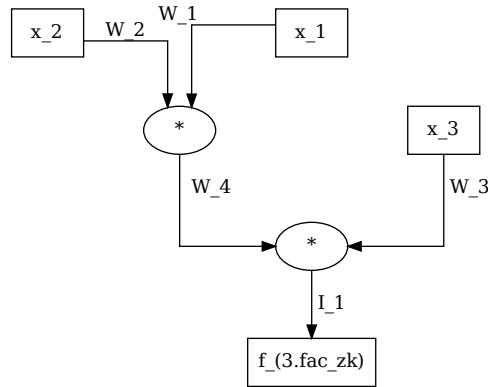
To understand the contribution of algebraic gates to the number of constraints, note that, by definition, multiplication gates have labels on their outgoing edges if and only if there is at least

one labeled edge in both input paths, or if the outgoing edge is an input to a sink node. This implies that multiplication with a constant is essentially free in the sense that it doesn't add a new constraint to the system, as long as that multiplication gate is not an input to an output node.

Moreover, addition gates have labels on their outgoing edges if and only if they are inputs to sink nodes. This implies that addition is essentially free in the sense that it doesn't add a new constraint to the system, as long as that addition gate is not an input to an output node.

*Example 123 (3-factorization).* Consider our 3-factorization problem from equation 6.8 and the associated circuit  $C_{3.fac}(\mathbb{F}_{13})$ . Our task is to transform this circuit into an equivalent rank-1 constraint system.

check  
reference



We start with an empty RICS, and, in order to generate all constraints, we have to iterate over the set of edge labels  $\{I_1; W_1, W_2, W_3, W_4\}$ .

Starting with the edge label  $I_1$ , we see that it is an outgoing edge of a multiplication gate, and, since both input edges are labeled, we have to add the following constraint to the system:

$$\begin{aligned} (\text{left input}) \cdot (\text{right input}) &= I_1 \\ W_4 \cdot W_3 &= I_1 \end{aligned} \quad \Leftrightarrow$$

Next, we consider the edge label  $W_1$  and, since, it's not an outgoing edge of a multiplication or addition label, we don't add a constraint to the system. The same holds true for the labels  $W_2$  and  $W_3$ .

For edge label  $W_4$ , we see that it is an outgoing edge of a multiplication gate, and, since both input edges are labeled, we have to add the following constraint to the system:

$$\begin{aligned} (\text{left input}) \cdot (\text{right input}) &= W_4 \\ W_2 \cdot W_1 &= W_4 \end{aligned} \quad \Leftrightarrow$$

Since there are no more labeled edges, all constraints are generated, and we have to combine them to get the associated RICS of  $C_{3.fac}(\mathbb{F}_{13})$ :

$$\begin{aligned} W_4 \cdot W_3 &= I_1 \\ W_2 \cdot W_1 &= W_4 \end{aligned}$$

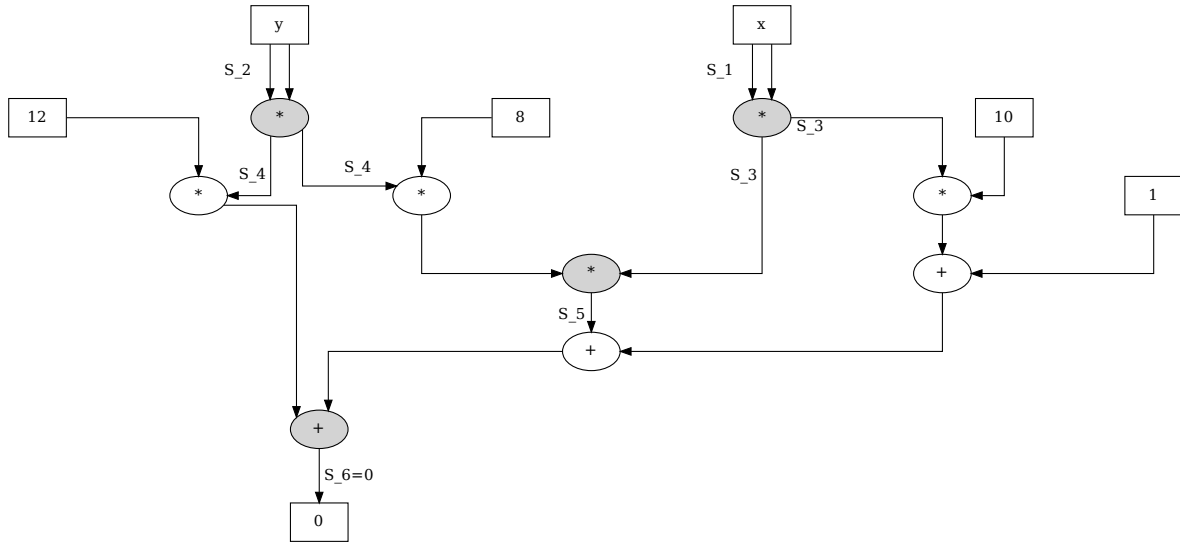
This system is equivalent to the RICS we derived in example 114. The languages  $L_{3.fac\_zk}$  and  $L_{3.fac\_circ}$  are therefore equivalent and both the circuit as well as the RICS are just two different ways of expressing the same language.

check  
reference

4723 *Example 124.* To consider a more general transformation, we consider the tiny-jubjub circuit  
 4724 from example 117 again. A proper circuit is given by

check  
reference

4725



4726

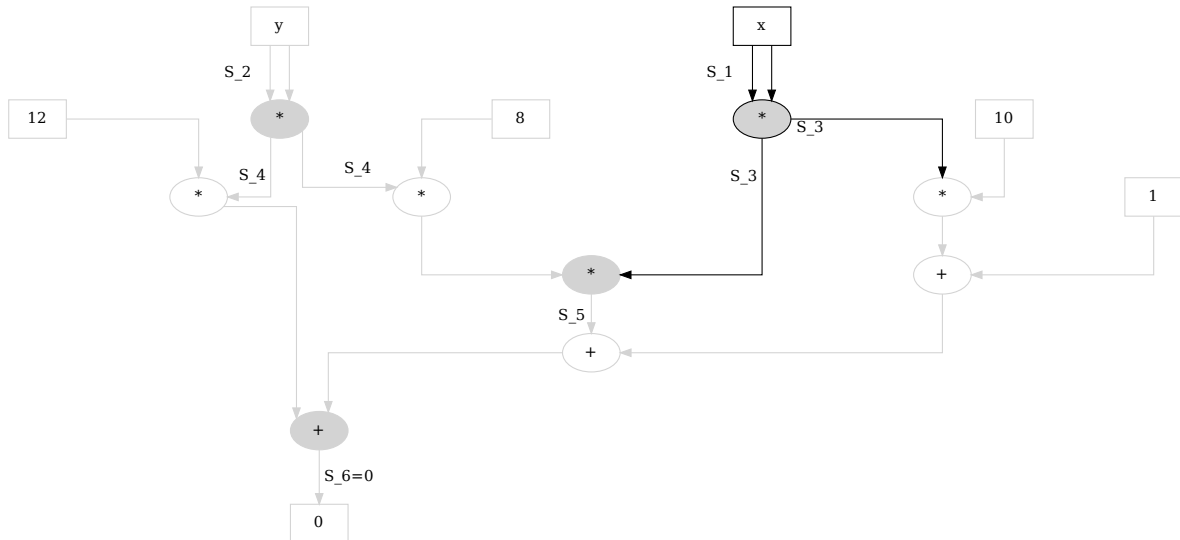
4727

4728 To compute the number of constraints, observe that we have 3 multiplication gates that have  
 4729 labels on their outgoing edges and 1 addition gate that has a label on its outgoing edge. We  
 4730 therefore have to compute 4 quadratic constraints.

4731 In order to derive the associated R1CS, we have start with an empty R1CS and then iterate  
 4732 over the set  $\{S_1, S_2, S_3, S_4, S_5, S_6 = 0\}$  of all edge labels, in order to generate the constraints.

4733 Considering edge label  $S_1$ , we see that the associated edges are not outgoing edges of any  
 4734 algebraic gate, and we therefore have to add no new constraint to the system. The same holds  
 4735 true for edge label  $S_2$ . Looking at edge label  $S_3$ , we see that the associated edges are outgoing  
 4736 edges of a multiplication gate and that the associated subgraph is given by:

4737



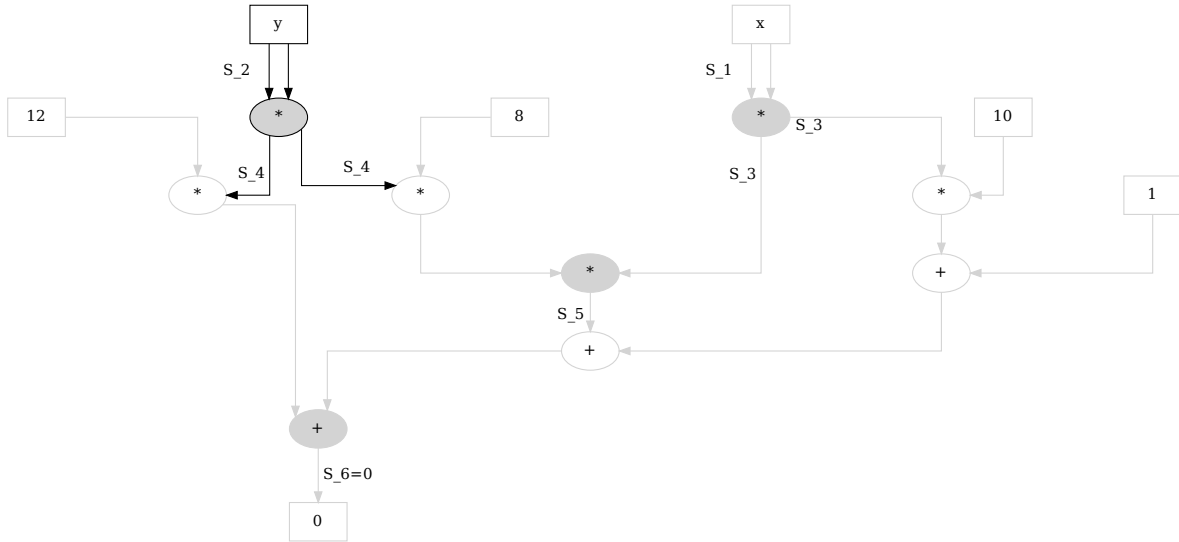
4738

4739

Both the left and the right input to this multiplication gate are labeled by  $S_1$ . We therefore have to add the following constraint to the system:

$$S_1 \cdot S_1 = S_3$$

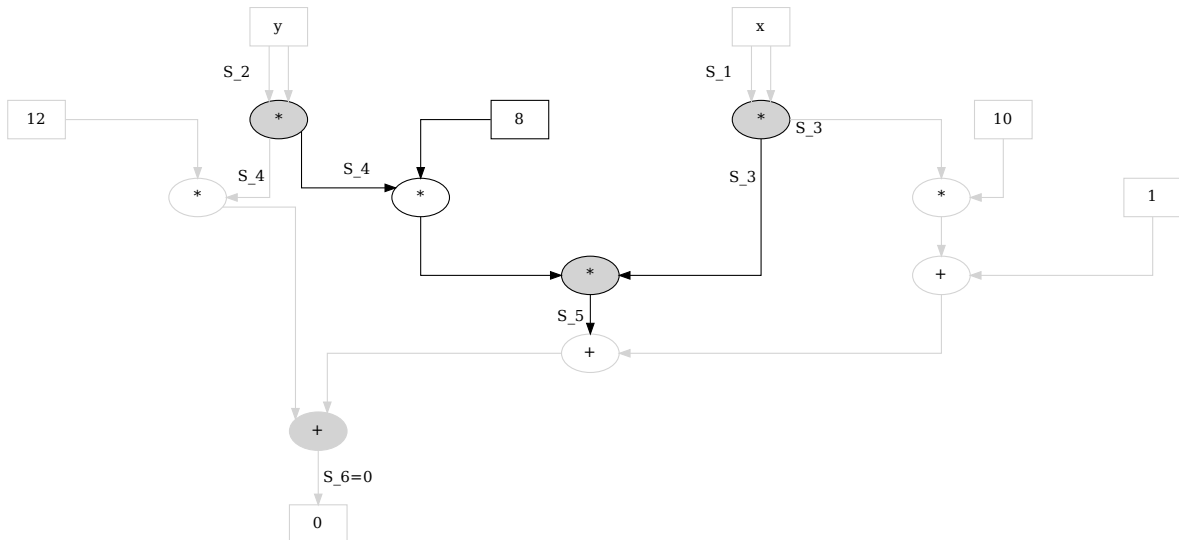
Looking at edge label  $S_4$ , we see that the associated edges are outgoing edges of a multiplication gate and that the associated subgraph is given by:



Both the left and the right input to this multiplication gate are labeled by  $S_2$  and we therefore have to add the following constraint to the system:

$$S_2 \cdot S_2 = S_4$$

Edge label  $S_5$  is more interesting. To see if it implies a constraint, we have to construct the associated subgraph first, which consists of all edges and all nodes in all path starting either at a constant input or a labeled edge. We get



4750

The right input to the associated multiplication gate is given by the labeled edge  $S_3$ . However, the left input is not a labeled edge, but has a labeled edge in one of its path. This implies that we have to add a constraint to the system. To compute the left factor of that constraint, we have to compute the output of subgraph associated to the left edge, which is  $8 \cdot W_2$ . This gives the constraint

$$(S_4 \cdot 8) \cdot S_3 = S_5$$

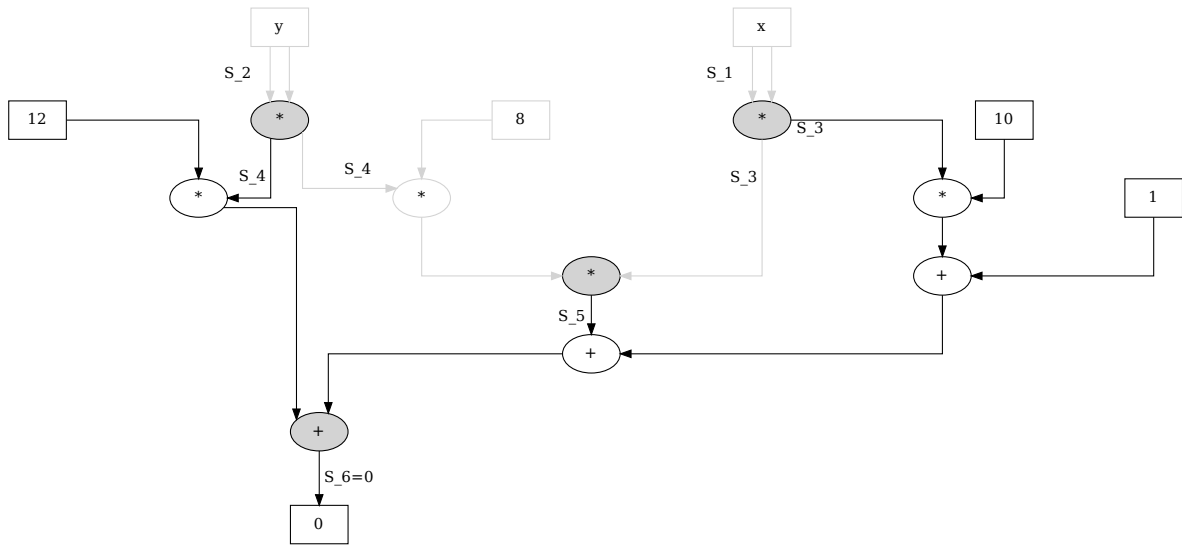
4751

4752

4753

The last edge label is the constant  $S_6 = 0$ . To see if it implies a constraint, we have to construct the associated subgraph, which consists of all edges and all nodes in all path starting either at a constant input or a labeled edge. We get

4754



4755

4756

Both the left and the right input are unlabeled, but have a labeled edges in their path. This implies that we have to add a constraint to the system. Since the gate is an addition gate, the right factor in the quadratic constraint is always 1 and the left factor is computed by symbolically executing all inputs to all gates in sub-circuit. We get

$$(12 \cdot S_4 + S_5 + 10 \cdot S_3 + 1) \cdot 1 = 0$$

Since there are no more labeled outgoing edges, we are done deriving the constraints. Combining all constraints together, we get the following R1CS:

$$S_1 \cdot S_1 = S_3$$

$$S_2 \cdot S_2 = S_4$$

$$(S_4 \cdot 8) \cdot S_3 = S_5$$

$$(12 \cdot S_4 + S_5 + 10 \cdot S_3 + 1) \cdot 1 = 0$$

4757

4758

4759

which is equivalent to the R1CS we derived in example 117. The languages  $L_{3, fac\_zk}$  and  $L_{3, fac\_circ}$  are therefore equivalent and both the circuit as well as the R1CS are just two different ways to express the same language.

check  
reference

### 6.2.3 Quadratic Arithmetic Programs

We have introduced algebraic circuits and their associated rank-1 constraints systems as two particular models able to represent space- and time-bounded computation. Both models define formal languages, and associated membership as well as knowledge claims can be constructively proved by executing the circuit in order to compute solutions to its associated RICS.

One reason why those systems are useful in the context of succinct zero-knowledge proof systems is because any RICS can be transformed into another computational model called **quadratic arithmetic programs** (QAP), which serve as the basis for some of the most efficient succinct non-interactive zero-knowledge proof generators that currently exist.

As we will see, proving statements for languages that have checking relations defined by quadratic arithmetic programs can be achieved by providing certain polynomials, and those proofs can be verified by checking a particular divisibility property.

**QAP representation** To understand what quadratic arithmetic programs are in detail, let  $\mathbb{F}$  be a field and  $R$  a rank-1 constraints system over  $\mathbb{F}$  such that the number of non-zero elements in  $\mathbb{F}$  is strictly larger than the number  $k$  of constraints in  $R$ . Moreover, let  $a_j^i, b_j^i$  and  $c_j^i \in \mathbb{F}$  for every index  $0 \leq j \leq n+m$  and  $1 \leq i \leq k$ , be the defining constants of the RICS and  $m_1, \dots, m_k$  be arbitrary, invertible and distinct elements from  $\mathbb{F}$ .

Then a **quadratic arithmetic program** [QAP] of the RICS is the following set of polynomials over  $\mathbb{F}$ :

$$QAP(R) = \left\{ T \in \mathbb{F}[x], \{A_j, B_j, C_j \in \mathbb{F}[x]\}_{h=0}^{n+m} \right\} \quad (6.12)$$

In the equation above,  $T(x) := \prod_{l=1}^k (x - m_l)$  is a polynomial of degree  $k$ , called the **target polynomial** of the QAP and  $A_j, B_j$  as well as  $C_j$  are the unique degree  $k-1$  polynomials defined by the following equation:

$$A_j(m_i) = a_j^i \quad B_j(m_i) = b_j^i \quad C_j(m_i) = c_j^i \quad j = 1, \dots, n+m+1, i = 1, \dots, k \quad (6.13)$$

Given some rank-1 constraint system, an associated quadratic arithmetic program is therefore nothing but a set of polynomials, computed from the constants in the RICS. To see that the polynomials  $A_j, B_j$  and  $C_j$  are uniquely defined by the equations in XXX, recall that a polynomial of degree  $k-1$  is completely determined on  $k$  evaluation points and the equation 4 precisely determines those  $k$  evaluation points.

Since we only consider polynomials over fields, Lagrange's interpolation method from 3.30 in chapter ?? can be used to derive the polynomials  $A_j, B_j$  and  $C_j$  from their defining equations XXX. A practical method to compute a QAP from a given RICS therefore consists of two steps. If the RICS consists of  $k$  constraints, first choose  $k$  invertible and mutually different points from the underlying field. Every choice defines a different QAP for the same RICS. Then use Lagrange's method and equation XXX to compute the polynomials  $A_j, B_j$  and  $C_j$  for every  $1 \leq j \leq k$ .

*Example 125* (Generalized factorization SNARK). To provide a better intuition of quadratic arithmetic programs and how they are computed from their associated rank-1 constraint systems, consider the language  $L_{3, fac\_zk}$  from example 109 and its associated RICS:

$$\begin{array}{ll} W_1 \cdot W_2 = W_4 & \text{constraint 1} \\ W_4 \cdot W_3 = I_1 & \text{constraint 2} \end{array}$$

In this example we want to transform this RICS into an associated QAP. In a first step, we have to compute the defining constants  $a_j^i, b_j^i$  and  $c_j^i$  of the RICS. According to XXX, we have

add reference

"by"?

check reference

check reference

add reference

add reference

check reference

add reference



$$\begin{array}{cccccc} a_0^1 = 0 & a_1^1 = 0 & a_2^1 = 1 & a_3^1 = 0 & a_4^1 = 0 & a_5^1 = 0 \\ a_0^2 = 0 & a_1^2 = 0 & a_2^2 = 0 & a_3^2 = 0 & a_4^2 = 0 & a_5^2 = 1 \end{array}$$

$$\begin{array}{cccccc} b_0^1 = 0 & b_1^1 = 0 & b_2^1 = 0 & b_3^1 = 1 & b_4^1 = 0 & b_5^1 = 0 \\ b_0^2 = 0 & b_1^2 = 0 & b_2^2 = 0 & b_3^2 = 0 & b_4^2 = 1 & b_5^2 = 0 \end{array}$$

$$\begin{array}{cccccc} c_0^1 = 0 & c_1^1 = 0 & c_2^1 = 0 & c_3^1 = 0 & c_4^1 = 0 & c_5^1 = 1 \\ c_0^2 = 0 & c_1^2 = 1 & c_2^2 = 0 & c_3^2 = 0 & c_4^2 = 0 & c_5^2 = 0 \end{array}$$

Since the R1CS is defined over the field  $\mathbb{F}_{13}$  and has two constraining equations, we need to choose two arbitrary but distinct elements  $m_1$  and  $m_2$  from  $\mathbb{F}_{13}$ . We choose  $m_1 = 5$ , and  $m_2 = 7$  and with this choice we get the target polynomial

$$\begin{aligned} T(x) &= (x - m_1)(x - m_2) && \# \text{ Definition of } T \\ &= (x - 5)(x - 7) && \# \text{ Insert our choice} \\ &= (x + 8)(x + 6) && \# \text{ Negatives in } \mathbb{F}_{13} \\ &= x^2 + x + 9 && \# \text{ expand} \end{aligned}$$

4794 Then we have to compute the polynomials  $A_j$ ,  $B_j$  and  $C_j$  by their defining equation from the  
4795 R1CS coefficients. Since the R1CS has two constraining equations, those polynomials are of  
4796 degree 1 and they are defined by their evaluation at the point  $m_1 = 5$  and the point  $m_2 = 7$ .

At point  $m_1$ , each polynomial  $A_j$  is defined to be  $a_j^1$  and at point  $m_2$ , each polynomial  $A_j$  is defined to be  $a_j^2$ . The same holds true for the polynomials  $B_j$  as well as  $C_j$ . Writing all these equations now, we get:

$$\begin{array}{cccccc} A_0(5) = 0, & A_1(5) = 0, & A_2(5) = 1, & A_3(5) = 0, & A_4(5) = 0, & A_5(5) = 0 \\ A_0(7) = 0, & A_1(7) = 0, & A_2(7) = 0, & A_3(7) = 0, & A_4(7) = 0, & A_5(7) = 1 \end{array}$$

$$\begin{array}{cccccc} B_0(5) = 0, & B_1(5) = 0, & B_2(5) = 0, & B_3(5) = 1, & B_4(5) = 0, & B_5(5) = 0 \\ B_0(7) = 0, & B_1(7) = 0, & B_2(7) = 0, & B_3(7) = 0, & B_4(7) = 1, & B_5(7) = 0 \end{array}$$

$$\begin{array}{cccccc} C_0(5) = 0, & C_1(5) = 0, & C_2(5) = 0, & C_3(5) = 0, & C_4(5) = 0, & C_5(5) = 1 \\ C_0(7) = 0, & C_1(7) = 1, & C_2(7) = 0, & C_3(7) = 0, & C_4(7) = 0, & C_5(7) = 0 \end{array}$$

4797 Lagrange's interpolation implies that a polynomial of degree  $k$ , that is, that zero on  $k + 1$  points  
4798 has to be the zero polynomial. Since our polynomials are of degree 1 and determined on 2  
4799 points, we therefore know that the only non-zero polynomials in our QAP are  $A_2$ ,  $A_5$ ,  $B_3$ ,  $B_4$ ,  
4800  $C_1$  and  $C_5$ , and that we can use Lagrange's interpolation to compute them.

To compute  $A_2$  we note that the set  $S$  in our version of Lagrange's method is given by  $S = \{(x_0, y_0), (x_1, y_1)\} = \{(5, 1), (7, 0)\}$ . Using this set we get:

$$\begin{aligned} A_2(x) &= y_0 \cdot l_0 + y_1 \cdot l_1 \\ &= y_0 \cdot \left( \frac{x - x_1}{x_0 - x_1} \right) + y_1 \cdot \left( \frac{x - x_0}{x_1 - x_0} \right) = 1 \cdot \left( \frac{x - 7}{5 - 7} \right) + 0 \cdot \left( \frac{x - 5}{7 - 5} \right) \\ &= \frac{x - 7}{-2} = \frac{x - 7}{11} && \# 11^{-1} = 6 \\ &= 6(x - 7) = 6x + 10 && \# -7 = 6 \text{ and } 6 \cdot 6 = 10 \end{aligned}$$

To compute  $A_5$ , we note that the set  $S$  in our version of Lagrange's method is given by  $S = \{(x_0, y_0), (x_1, y_1)\} = \{(5, 0), (7, 1)\}$ . Using this set we get:

$$\begin{aligned}
 A_5(x) &= y_0 \cdot l_0 + y_1 \cdot l_1 \\
 &= y_0 \cdot \left(\frac{x - x_1}{x_0 - x_1}\right) + y_1 \cdot \left(\frac{x - x_0}{x_1 - x_0}\right) = 0 \cdot \left(\frac{x - 7}{5 - 7}\right) + 1 \cdot \left(\frac{x - 5}{7 - 5}\right) \\
 &= \frac{x - 5}{2} & \# 2^{-1} = 7 \\
 &= 7(x - 5) = 7x + 4 & \# -5 = 8 \text{ and } 7 \cdot 8 = 4
 \end{aligned}$$

4801 Using Lagrange's interpolation, we can deduce that  $A_2 = B_3 = C_5$  as well as  $A_5 = B_4 = C_1$ ,  
 4802 since they are polynomials of degree 1 that evaluate to same values on 2 points. Using this, we  
 4803 get the following set of polynomials

$A_0(x) = 0$	$B_0(x) = 0$	$C_0(x) = 0$
$A_1(x) = 0$	$B_1(x) = 0$	$C_1(x) = 7x + 4$
$A_2(x) = 6x + 10$	$B_2(x) = 0$	$C_2(x) = 0$
$A_3(x) = 0$	$B_3(x) = 6x + 10$	$C_3(x) = 0$
$A_4(x) = 0$	$B_4(x) = 7x + 4$	$C_4(x) = 0$
$A_5(x) = 7x + 4$	$B_5(x) = 0$	$C_5(x) = 6x + 10$

4805 We can invoke Sage to verify our computation. In sage every polynomial ring has a function  
 4806 `lagrange_polynomial` that takes the defining points as inputs and the associated Lagrange  
 4807 polynomial as output.

```

4808 sage: F13 = GF(13)
4809 sage: F13t.<t> = F13[]
4810 sage: T = F13t((t-5)*(t-7))
4811 sage: A2 = F13t.lagrange_polynomial([(5, 1), (7, 0)])
4812 sage: A5 = F13t.lagrange_polynomial([(5, 0), (7, 1)])
4813 sage: T == F13t(t^2 + t + 9)
4814 True
4815 sage: A2 == F13t(6*t + 10)
4816 True
4817 sage: A5 == F13t(7*t + 4)
4818 True

```

4819 Combining this computation with the target polynomial we derived earlier, a quadratic arith-  
 4820 metic program associated to the rank-1 constraint system  $R_{3.fac\_zk}$  is given as follows:

$$\begin{aligned}
 QAP(R_{3.fac\_zk}) &= \{x^2 + x + 9, \\
 \{0, 0, 6x + 10, 0, 0, 7x + 4\}, \{0, 0, 0, 6x + 10, 7x + 4, 0\}, \{0, 7x + 4, 0, 0, 0, 6x + 10\}\}
 \end{aligned} \tag{6.14}$$

4821 **QAP Satisfiability** One of the major points of quadratic arithmetic programs in proofing sys-  
 4822 tems is that solutions of their associated rank-1 constraints systems are in 1:1 correspondence  
 4823 with certain polynomials  $P$  such that  $P$  is divisible by the target polynomial  $T$  of the QAP if and  
 4824 only if the solution is a solution. Verifying solutions to the R1CS and hence, checking proper  
 4825 circuit execution is then achievable by polynomial division of  $P$  by  $T$ .

4826 To be more specific, let  $R$  be some rank-1 constraints system with associated assignment  
 4827 variables  $(I_1, \dots, I_n; W_1, \dots, W_m)$  and let  $QAP(R)$  be a quadratic arithmetic program of  $R$ . Then

clarify  
language

the tuple  $(I_1, \dots, I_n; W_1, \dots, W_m)$  is a solution to the R1CS if and only if the following polynomial is divisible by the target polynomial  $T$ :

$$P_{(I;W)} = (A_0 + \sum_j^n I_j \cdot A_j + \sum_j^m W_j \cdot A_{n+j}) \cdot (B_0 + \sum_j^n I_j \cdot B_j + \sum_j^m W_j \cdot B_{n+j}) - (C_0 + \sum_j^n I_j \cdot C_j + \sum_j^m W_j \cdot C_{n+j}) \quad (6.15)$$

Every tuple  $(I; W)$  defines a polynomial  $P_{(I;W)}$ , and, since each polynomial  $A_j$ ,  $B_j$  and  $C_j$  is of degree  $k-1$ ,  $P_{(I;W)}$  is of degree  $(k-1) \cdot (k-1) = k^2 - 2k + 1$ .

To understand how quadratic arithmetic programs define formal languages, observe that every QAP over a field  $\mathbb{F}$  defines a decision function over the alphabet  $\Sigma_I \times \Sigma_W = \mathbb{F} \times \mathbb{F}$  in the following way:

$$R_{QAP} : \mathbb{F}^* \times \mathbb{F}^* \rightarrow \{true, false\} ; (I; W) \mapsto \begin{cases} true & P_{(I;W)} \text{ is divisible by } T \\ false & \text{else} \end{cases} \quad (6.16)$$

This means that every QAP defines a formal language, and, if the QAP is associated to an R1CS, it can be shown that the two languages are equivalent. A **statement** is a membership claim “There is a word  $(I; W)$  in  $L_{QAP}$ ”. A proof to this claim is therefore a polynomial  $P_{(I;W)}$ , which is verified by dividing  $P_{(I;W)}$  by  $T$ .

Note the structural similarity to the definition of an R1CS in 6.2.1.1 and the different ways of computing proofs in both systems. For circuits and their associated rank-1 constraints systems, a constructive proof consists of a valid assignment of field elements to the edges of the circuit, or the variables in the R1CS. However, in the case of QAPs, a valid proof consists of a polynomial  $P_{(I;W)}$ .

To compute a proof for a statement in  $L_{QAP}$  given some instance  $I$ , a proofer first needs to compute a constructive proof  $W$ , e.g. by executing the circuit. With  $(I; W)$  at hand, the proofer can then compute the polynomial  $P_{(I;W)}$  and publish it as proof.

Verifying a constructive proof in the case of a circuit is achieved by executing the circuit, comparing the result to the given proof, and verifying the same proof in the R1CS picture means checking if the elements of the proof satisfy all equation.

In contrast, verifying a proof in the case of a QAP is done by polynomial division of the proof  $P$  by the target polynomial  $T$  of the QAP. The proof checks out if and only if  $P$  is divisible by  $T$ .

*Example 126.* Consider the quadratic arithmetic program  $QAP(R_{3, fac\_zk})$  from example XXX, and its associated R1CS from equation 6.1.0.1. To give an intuition of how proofs in the language  $L_{QAP(R_{3, fac\_zk})}$  let's consider the instance  $I_1 = 11$ . As we know from example XXX,  $(W_1, W_2, W_3, W_5) = (2, 3, 4, 6)$  is a proper witness, since  $(I_1; W_1, W_2, W_3, W_5) = (11; 2, 3, 4, 6)$  is a valid circuit assignment and hence, a solution to  $R_{3, fac\_zk}$  and a constructive proof for language  $L_{R_{3, fac\_zk}}$ .

In order to transform this constructive proof into a membership proof in language  $L_{QAP(R_{3, fac\_zk})}$  a proofer has to use the elements of the constructive proof, to compute the polynomial  $P_{(I;W)}$ .

In the case of  $(I_1; W_1, W_2, W_3, W_5) = (11; 2, 3, 4, 6)$ , the associated proof is computed as fol-

check  
reference

add refer-  
ence

check  
reference

add refer-  
ence

lows:

$$\begin{aligned}
P_{(I;W)} &= (A_0 + \sum_j^n I_j \cdot A_j + \sum_j^m W_j \cdot A_{n+j}) \cdot (B_0 + \sum_j^n I_j \cdot B_j + \sum_j^m W_j \cdot B_{n+j}) - (C_0 + \sum_j^n I_j \cdot C_j + \sum_j^m W_j \cdot C_{n+j}) \\
&= (2(6x + 10) + 6(7x + 4)) \cdot (3(6x + 10) + 4(7x + 4)) - (11(7x + 4) + 6(6x + 10)) \\
&= ((12x + 7) + (3x + 11)) \cdot ((5x + 4) + (2x + 3)) - ((12x + 5) + (10x + 8)) \\
&= (2x + 5) \cdot (7x + 7) - (9x) \\
&= (x^2 + 2 \cdot 7x + 5 \cdot 7x + 5 \cdot 7) - (9x) \\
&= (x^2 + x + 9x + 9) - (9x) \\
&= x^2 + x + 9
\end{aligned}$$

4861 Given instance  $I_1 = 11$  a proofer therefore provides the polynomial  $x^2 + x + 9$  as proof. To verify  
 4862 this proof, any verifier can then look up the target polynomial  $T$  from the QAP and divide  $P_{(I;W)}$   
 4863 by  $T$ . In this particular example,  $P_{(I;W)}$  is equal to the target polynomial  $T$ , and hence, it is  
 4864 divisible by  $T$  with  $P/T = 1$ . The verification therefore checks the proof.

```

4865 sage: F13 = GF(13) 660
4866 sage: F13t.<t> = F13[] 661
4867 sage: T = F13t(t^2 + t + 9) 662
4868 sage: P = F13t((2*(6*t+10)+6*(7*t+4))*(3*(6*t+10)+4*(7*t+4)) 663
4869             -(11*(7*t+4)+6*(6*t+10)))
4870 sage: P == T 664
4871 True 665
4872 sage: P % T # remainder 666
4873 0 667

```

To give an example of a false proof, consider the tuple  $(I_1; W_1, W_2, W_3, W_4) = (11, 2, 3, 4, 8)$ . Executing the circuit, we can see that this is not a valid assignment and not a solution to the R1CS, and hence, not a constructive knowledge proof in  $L_{3.fac\_zk}$ . However, a proofer might use these values to construct a false proof  $P_{(I;W)}$ :

$$\begin{aligned}
P'_{(I;W)} &= (A_0 + \sum_j^n I_j \cdot A_j + \sum_j^m W_j \cdot A_{n+j}) \cdot (B_0 + \sum_j^n I_j \cdot B_j + \sum_j^m W_j \cdot B_{n+j}) - (C_0 + \sum_j^n I_j \cdot C_j + \sum_j^m W_j \cdot C_{n+j}) \\
&= (2(6x + 10) + 8(7x + 4)) \cdot (3(6x + 10) + 4(7x + 4)) - (8(6x + 10) + 11(7x + 4)) \\
&= 8x^2 + 6
\end{aligned}$$

Given instance  $I_1 = 11$ , a proofer therefore provides the polynomial  $8x^2 + 6$  as proof. To verify this proof, any verifier can look up the target polynomial  $T$  from the QAP and divide  $P_{(I;W)}$  by  $T$ . However, polynomial division has the following remainder:

$$(8x^2 + 6)/(x^2 + x + 9) = 8 + \frac{5x + 12}{x^2 + x + 9}$$

4874 This implies that  $P_{(I;W)}$  is not divisible by  $T$ , and hence, the verification does not check the  
 4875 proof. Any verifier can therefore show that the proof is false.

```

4876 sage: F13 = GF(13) 668
4877 sage: F13t.<t> = F13[] 669
4878 sage: T = F13t(t^2 + t + 9) 670
4879 sage: P = F13t((2*(6*t+10)+8*(7*t+4))*(3*(6*t+10)+4*(7*t+4))-( 671
4880             8*(6*t+10)+11*(7*t+4)))

```

4881	<code>sage: P == F13t(8*t^2 + 6)</code>	672
4882	<code>True</code>	673
4883	<code>sage: P % T # remainder</code>	674
4884	<code>5*t + 12</code>	675

# Chapter 7

## Circuit Compilers

As we have seen in the previous chapter, statements can be formalized as membership or knowledge claims in formal language, and algebraic circuits as well as rank-1 constraint systems are two practically important ways to define those languages.

However, both algebraic circuits and rank-1 constraint systems are not ideal from a developers point of view, because they deviate substantially from common programming paradigms. Writing real-world applications as circuits and the associated verification in terms of rank-1 constraint systems is at least as troublesome as writing any other low-level language like assembler code. To allow for complex statement design, it is therefore necessary to have some kind of compiler framework, capable of transforming high-level languages into arithmetic circuits and associated rank-1 constraint systems.

As we have seen in chapter 6 and in 6.2.1.1., both arithmetic circuits and rank-1 constraint systems have a modularity property by which it is possible to synthesize complex circuits from simple ones. A basic approach taken by many circuit/R1CS compilers is therefore to provide a library of atomic and simple circuits and then define a way to combine those basic building blocks into arbitrary complex systems.

In this chapter, we provide an introduction to basic concepts of so-called **circuit compilers** and derive a toy language which we can “compile” in a pen-and-paper approach into algebraic circuits and their associated rank-1 constraint systems.

We start with a general introduction to our language, and then introduce atomic types like booleans and unsigned integers. Then we define the fundamental control flow primitives like the if-then-else conditional and the bounded loop. We will look at basic functionality primitives like elliptic curve cryptography. Primitives like these are often called **gadgets** in the literature.

### 7.1 A Pen-and-Paper Language

To explain basic concepts of circuit compilers and their associated high-level languages, we derive an informal toy language and associated “brain-compiler” which we name PAPER (**Pen-And-Paper Execution Rules**). PAPER allows programmers to define statements in Rust-like pseudo-code. The language is inspired by ZOKRATES and `circom`.

#### 7.1.1 The Grammar

In PAPER, any statement is defined as an ordered list of functions, where any function has to be declared in the list before it is called in another function of that list. The last entry in a statement has to be a special function, called `main`. Functions take a list of typed parameters as inputs

check  
references

add refer-  
ences to  
these lan-  
guages?

and compute a tuple of typed variables as output, where types are special functions that define how to transform that type into another type, ultimately transforming any type into elements of the base field where the circuit is defined over.

Any statement is parameterized over the field that the circuit will be defined on, and has additional optional parameters of unsigned type, needed to define the size of array or the counter of bounded loops. The following definition makes the grammar of a statement precise using a command line language like description:

```
statement <Name> {F:<Field> [ , <N_1: unsigned>, ... ] } {
  [fn <Name>([[pub]<Arg>:<Type>, ...]) -> (<Type>, ...)] {
    [let [pub] <Var>:<Type> ; ... ]
    [let const <Const>:<Type>=<Value> ; ... ]
    Var<==>(fn ([<Arg>|<Const>|<Var>, ...]) | (<Arg>|<Const>|<Var>)) ;
    return (<Var>, ...) ;
  } ; ...]
  fn main([[pub]<Arg>:<Type>, ...]) -> (<Type>, ...) {
    [let [pub] <Var>:<Type> ; ... ]
    [let const <Const>:<Type>=<Value> ; ... ]
    Var<==>(fn ([<Arg>|<Const>|<Var>, ...]) | (<Arg>|<Const>|<Var>)) ;
    return (<Var>, ...) ;
  } ;
}
```

Function arguments and variables are private by default, but can be declared as public by the `pub` specifier. Declaring arguments and variables as public always overwrites any previous or conflicting private declarations. Every argument, constant or variable has a type, and every type is defined as a function that transforms that type into another type:

```
type <TYPE>( t1 : <TYPE_1>) -> TYPE_2{
  let t2: TYPE_2 <== fn(TYPE_1)
  return t2
}
```

Many real-world circuit languages are based on a similar, but of course more sophisticated approach than PAPER. The purpose of PAPER is to show basic principles of circuit compilers and their associated high-level languages.

*Example 127.* To get a better understanding of the grammar of PAPER, the following constitutes proper high-level code that follows the grammar of the PAPER language, assuming that all types in that code have been defined elsewhere.

```
statement MOCK_CODE {F: F_43, N_1 = 1024, N_2 = 8} {
  fn foo(in_1 : F, pub in_2 : TYPE_2) -> F {
    let const c_1 : F = 0 ;
    let const c_2 : TYPE_2 = SOME_VALUE ;
    let pub out_1 : F ;
    out_1<== c_1 ;
    return out_1 ;
  } ;

  fn bar(pub in_1 : F) -> F {
    let out_1 : F ;
    out_1<==foo(in_1);
    return out_1 ;
  } ;
}
```

```

4966   } ;
4967
4968   fn main(in_1 : TYPE_1) -> (F, TYPE_2) {
4969       let const c_1 : TYPE_1 = SOME_VALUE ;
4970       let const c_2 : F = 2;
4971       let const c_3 : TYPE_2 = SOME_VALUE ;
4972       let pub out_1 : F ;
4973       let out_2 : TYPE_2 ;
4974       c_1 <== in_1 ;
4975       out_1 <== foo(c_2) ;
4976       out_2 <== TYPE_2 ;
4977       return (out_1, out_2) ;
4978   } ;
4979 }

```

### 7.1.2 The Execution Phases

In contrast to normal executable programs, programs for circuit compilers have two modes of execution. The first mode, usually called the **setup phase**, is executed in order to generate the circuit and its associated rank-1 constraint system, the latter of which is then usually used as input to some zero-knowledge proof system.

The second mode of execution is usually called the **prover phase**. In this phase, a prover usually computes a valid assignment to the circuit. Depending on the use case, this valid assignment is then either directly used as constructive proof for proper circuit execution or is transferred as input to the proof generation algorithm of some zero-knowledge proof system, where the full-sized, non hiding constructive proof is processed into a succinct proof with various levels of zero knowledge.

Modern circuit languages and their associated compilers abstract over those two phases and provide a unified **interphase** to the developer, who then writes a single program that can be used in both phases.

To give the reader a clear, conceptual distinction between the two phases, PAPER keeps them separated. Code can be “brain-compiled” during the **setup-phase** in a pen-and-paper approach into visual circuits. Once a circuit is derived, it can be executed in a **prover phase** to generate a valid assignment. The valid assignment is then interpreted as a constructive proof for a knowledge claim in the associated language.

**The Setup Phase** In PAPER, the task of the setup phase is to compile code in the PAPER language into a visual representation of an algebraic circuit. Deriving the circuit from the code in a pen-and-paper style is what we call **brain-compiling**.

Given some statement description that adheres to the correct grammar, we start circuit development with an empty circuit, compile the main function first and then inductively compile all other functions as they are called during the process.

For every function we compile, we draw a box-node for every argument, every variable and every constant of that function. If the node represents a variable, we label it with that variable’s name, and if it represents a constant, we label it with that constant’s value. We group arguments into a subgraph labeled “inputs” and return values into a subgraph labeled “outputs”. We then group everything into a subgraph and label that subgraph with the function’s name.

After this is done, we have to do a consistency and type check for every occurrence of the



assignment operator `<==`. We have to ensure that the expression on the right side of the operator is well defined and that the types of both side match.

Then we compile the right side of every occurrence of the assignment operator `<==`. If the right side is a constant or variable defined in this function, we draw a dotted line from the box-node that represents the left side of `<==` to the box node that represents the right side of the same operator. If the right side represents an argument of that function we draw a line from the box-node that represents the left side of `<==` to the box node that represents the right side of the same operator.

If the right side of the `<==` operator is a function, we look into our database, find its associated circuit and draw it. If no circuit is associated to that function yet, we repeat the compilation process for that function, drawing edges from the function's argument to its input nodes and from the functions output nodes to the nodes on the right side of `<==`.

During that process, edge labels are drawn according to the rules from 6.2.2.1. If the associated variable represents a private value, we use the *W* label to indicate a witness, and if it represents a public value, we use the *I* label to indicate an instance.

check  
reference

Once this is done, we compile all occurring types in a function, by compiling the function of each type. We do this inductively until we reach the type of the base field. Circuits have no notion of types, only of field elements; hence, every type needs to be compiled to the field type in a sequence of compilation steps.

The compilation stops once we have inductively replaced all functions by their circuits. The result is a circuit that contains many unnecessary box nodes. In a final optimization step, all box nodes that are directly linked to each other are collapsed into a single node, and all box nodes that represent the same constants are collapsed into a single node.

Of course, PAPER's brain-compiler is not properly defined in any formal manner. Its purpose is to highlight important steps that real-world compilers undergo in their setup phases.

*Example 128 (A trivial Circuit).* To give an intuition of how to write and compile circuits in the PAPER language, consider the following statement description:

```
statement trivial_circuit {F:F_13} {
  fn main{F}(in1 : F, pub in2 : F) -> (F,F) {
    let const outc1 : F = 0 ;
    let const incl : F = 7 ;
    let out1 : F ;
    let out2 : F ;
    out1 <== incl;
    out2 <== in1;
    outc1 <== in2;
    return (out1, out2) ;
  }
}
```

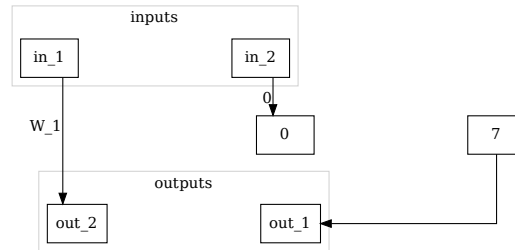
To brain-compile this statement into an algebraic circuit with PAPER, we start with an empty circuit and evaluate function `main`, which is the only function in this statement.

We draw box-nodes for every argument, every constant and every variable of the function and label them with their names or values, respectively. Then we do a consistency and type check for every `<==` operator in the function. Since the circuit only wires inputs to outputs and all elements have the same type, the check is valid.

Then we evaluate the right side of the assignment operators. Since, in our case, the right side of each operator is not a function, we draw edges from the box-nodes on the right side to the associated box node on the left side. To label those edges, we use the general rules of

algebraic circuits as defined in 6.2.2.1. According to those rules, every incoming edge of a sink node has a label and every outgoing edge of a source node has a label, if the node is labeled with a variable. Since nodes that represent constants are implicitly assumed to be private, and since the public specifier determines if an edge is labeled with  $W$  or  $I$ , we get the following circuit:

check  
reference



**The Prover Phase** In PAPER, a so-called **prover phase** can be executed once the setup phase has generated a circuit image from its associated high-level code. This is done by executing the circuit while assigning proper values to all input nodes of the circuit. However, in contrast to most real-world compilers, PAPER does not tell the prover how to find proper input values to a given circuit. Real-world programming languages usually provide this data by computations that are done outside of the circuit.

*Example 129.* Consider the circuit from example 128. Valid assignments to this circuit are constructive proofs that the pair of inputs  $(S_1, S_2)$  is a point on the tiny-jubjub curve. However, the circuit does not provide a way to actually compute proper values for  $S_1$  and  $S_2$ . Any real-world system therefore needs an auxiliary computation that provides those values.

check  
reference

## 7.2 Common Programing concepts

In this section, we cover concepts that appear in almost every programming language, and see how they can be implemented in circuit compilers.

### 7.2.1 Primitive Types

Primitive data types like booleans, (unsigned) integers, or strings are the most basic building blocks one can expect to find in every general high-level programming language. In order to write statements as computer programs that compile into circuits, it is therefore necessary to implement primitive types as constraint systems, and define their associated operations as circuits.

In this section, we look at some common ways to achieve this. After a recapitulation of the atomic type of prime field elements, we start with an implementation of the boolean type and its associated boolean algebra as circuits. After that, we define unsigned integers based on the boolean type, and leave the implementation of signed integers as an exercise to the reader.

It should be noted, however, that while primitive data types in common programming languages (like C, Go, or Rust) have a one-to-one correspondence with objects in the computer's memory, this is not the case for most languages that compile into algebraic circuits. As we will see in the following paragraphs, common primitives like booleans or unsigned integers require many constraints and memory. Primitives different from the underlying field elements can be expensive.

### The base-field type

Since both algebraic circuits and their associated rank-1 constraint systems are defined over a finite field, elements from that field are the atomic informational units in those models. In this sense, field elements  $x \in \mathbb{F}$  are for algebraic circuits what bits are for computers.

In PAPER, we write  $\mathbb{F}$  for this type and specify the actual field instance for every statement in curly brackets after the name of that statement. Two functions are associated to this type, which are induced by the **addition** and **multiplication** law in the field  $\mathbb{F}$ . We write

$$\text{MUL} : \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F} ; (x, y) \mapsto \text{MUL}(x, y) \quad (7.1)$$

$$\text{ADD} : \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F} ; (x, y) \mapsto \text{ADD}(x, y) \quad (7.2)$$

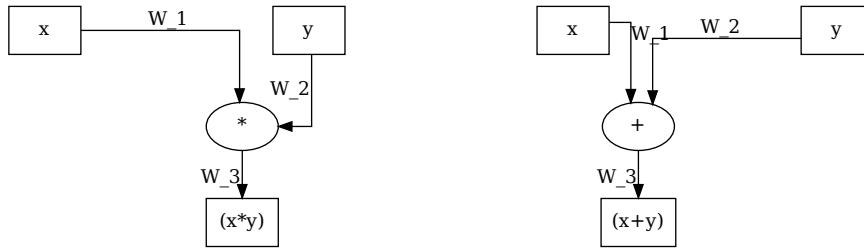
Circuit compilers have to compile these functions into algebraic gates, as explained in 6.2.2.2. Every other function has to be expressed in terms of them and proper wiring.

To represent addition and multiplication in the PAPER language, we define the following two functions:

```
fn MUL(x : F, y : F) -> (MUL(x, y) : F) {}
```

```
fn ADD(x : F, y : F) -> (ADD(x, y) : F) {}
```

The compiler then compiles every occurrence of the MUL or the ADD function into the following circuits:



*Example 130 (Basic gates).* To give an intuition of how a real-world compiler might transform addition and multiplication in algebraic expressions into a circuit, consider the following PAPER statement:

```
statement basic_ops {F:F_13} {
  fn main(in_1 : F, pub in_2 : F) -> (out_1:F, out_2:F) {
    out_1 <== MUL(in_1, in_2) ;
    out_2 <== ADD(in_1, in_2) ;
  }
}
```

To compile this into an algebraic circuit, we start with an empty circuit and evaluate the function `main`, which is the only function in this statement.

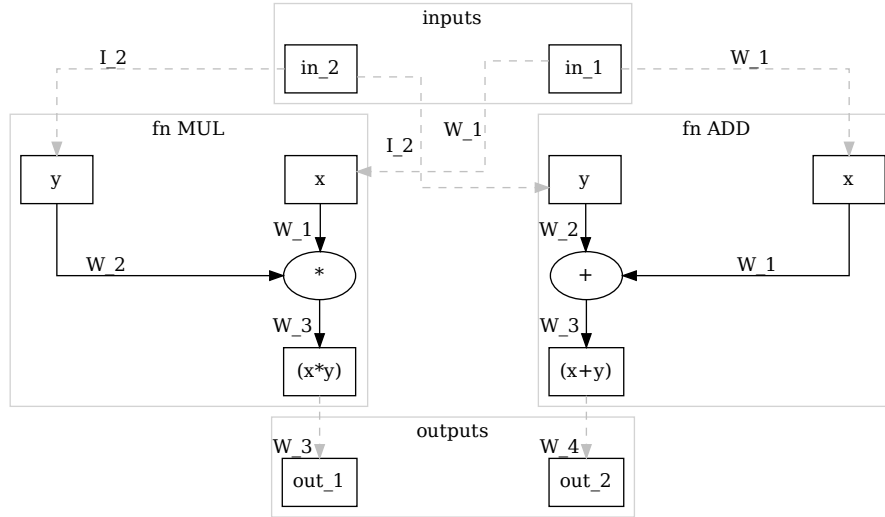
We draw an inputs subgraph containing box-nodes for every argument of the function, and an outputs subgraph containing box-nodes for every factor in the return value. Since all of these nodes represent variables of the `field` type, we don't have to add any type constraints to the circuit.

We check the validity of every expression on the right side of every `<==` operator including a type check. In our case, every variable is of the `field` type and hence the types match the types of the `MUL` as well as the `ADD` function and the type of the left sides of `<==` operators.

check  
reference

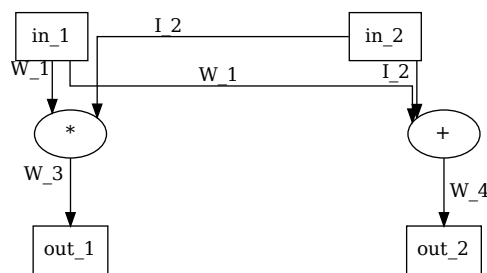
We evaluate the expressions on the right side of every `<==` operator inductively, replacing every occurrence of a function with a subgraph that represents its associated circuit.

According to PAPER, every occurrence of the `public` specifier overwrites the associate `private` default value. Using the appropriate edge labels we get:



Any real-world compiler might process its associated high-level language in a similar way, replacing functions, or gadgets by predefined associated circuits. This process is often followed by various optimization steps that try to reduce the number of constraints as much as possible.

In PAPER, we optimize this circuit by collapsing all box nodes that are directly connected to other box nodes, adhering to the rule that a variable's `public` specifier overwrites any `private` specifier. Reindexing edge labels, we get the following circuit as our pen and pencil compiler output:



*Example 131 (3-factorization).* Consider our 3-factorization problem from example 109 and the associated circuit  $C_{3.\text{fac\_zk}}(\mathbb{F}_{13})$  we provided in equation 6.8. To understand the process of replacing high-level functions by their associated circuits inductively, we want define a PAPER statement that we brain-compile into an algebraic circuit equivalent to  $C_{3.\text{fac\_zk}}(\mathbb{F}_{13})$ :

```
statement 3_fac_zk {F:F_13} {
  fn main(x_1 : F, x_2 : F, x_3 : F) -> (pub 3_fac_zk : F) {
    f_3.fac_zk <== MUL( MUL( x_1 , x_2 ) , x_3 ) ;
  }
}
```

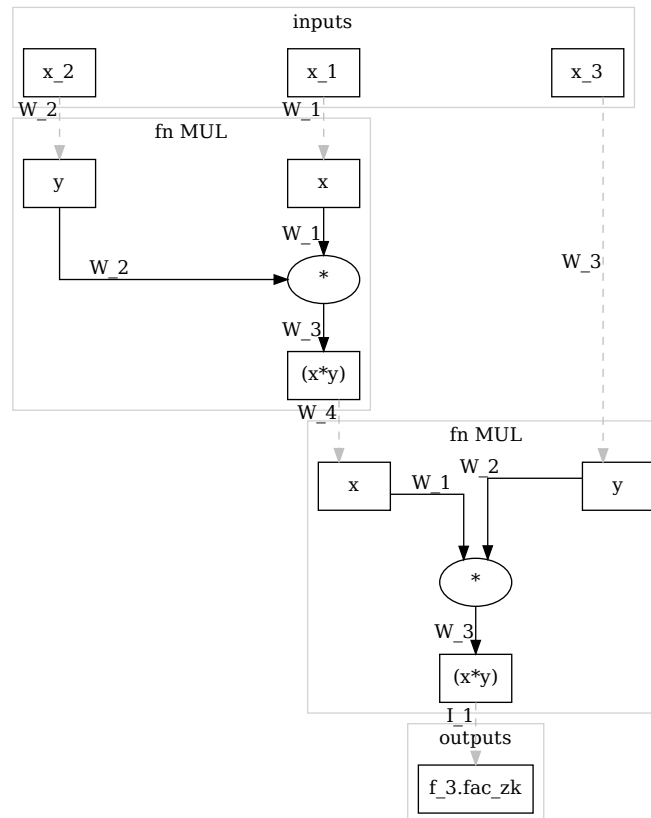
check  
reference

check  
reference

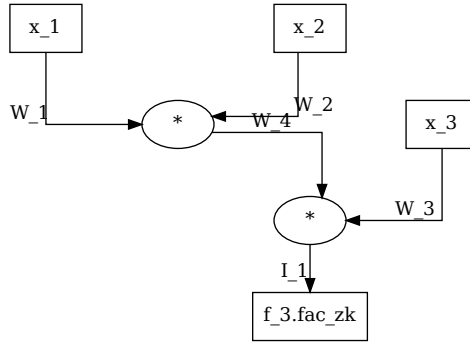
Using PAPER, we start with an empty circuit and then add 3 input nodes to the input subgraph as well as 1 output node to the output subgraph. All these nodes are decorated with the associated variable names. Since all of these nodes represent variables of the `field` type, we don't have to add any type constraints to the circuit.

We check the validity of every expression on the right side of the single `<==` operator including a type check.

We evaluate the expressions on the right side of every `<==` operator inductively. We have two nested multiplication functions and we replace them by the associated multiplication circuits, starting with the most outer function. We get:



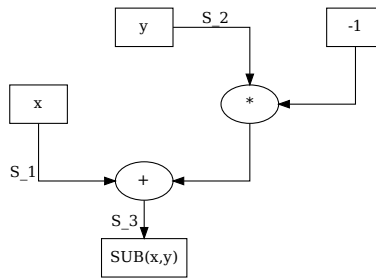
In a final optimization step, we collapse all box nodes directly connected to other box nodes, adhering to the rule that a variable's `public` specifier overwrites any `private` specifier. Reindexing edge labels we get the following circuit:



5162

5163 **The Subtraction Constraint System** By definition, algebraic circuits only contain addition  
 5164 and multiplication gates, and it follows that there is no single gate for field subtraction, despite  
 5165 the fact that subtraction is a native operation in every field.

5166 High-level languages and their associated circuit compilers, therefore, need another way to  
 5167 deal with subtraction. To see how this can be achieved, recall that subtraction is defined by addi-  
 5168 tion with the additive inverse, and that the inverse can be computed efficiently by multiplication  
 5169 with  $-1$ . A circuit for field subtraction is therefore given by



5170

5171 Using the general method from 6.2.1.1, the circuits associated rank-1 constraint system is given  
 5172 by:

$$(S_1 + (-1) \cdot S_2) \cdot 1 = S_3 \quad (7.3)$$

5173 Any valid assignment  $\{S_1, S_2, S_3\}$  to this circuit therefore enforces the value  $S_3$  to be the differ-  
 5174 ence  $S_1 - S_2$ .

5175 Real-world compilers usually provide a gadget or a function to abstract over this circuit  
 5176 such that programers can use subtraction as if it were native to circuits. In PAPER, we define  
 5177 the following subtraction function that compiles to the previous circuit:

```
5178 fn SUB(x : F, y : F) -> (SUB(x,y) : F) {
5179   constant c : F = -1 ;
5180   SUB <== ADD(x , MUL( y , c ) );
5181 }
```

5182 In the setup phase of a statement, we compile every occurrence of the SUB function into an  
 5183 instance of its associated subtraction circuit, and edge labels are generated according to the  
 5184 rules from 6.2.2.1.

check  
reference

check  
reference

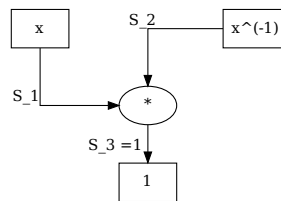
**The Inversion Constraint System** By definition, algebraic circuits only contain addition and multiplication gates, and it follows that there is no single gate for field inversion, despite the fact that inversion is a native operation in every field.

If the underlying field is a prime field, one approach would be to use Fermat’s little theorem 3.3 to compute the multiplicative inverse inside the circuit. To see how this works, let  $\mathbb{F}_p$  be the prime field. The multiplicative inverse  $x^{-1}$  of a field element  $x \in \mathbb{F}$  with  $x \neq 0$  is then given by  $x^{-1} = x^{p-2}$ , and computing  $x^{p-2}$  in the circuit therefore computes the multiplicative inverse.

Unfortunately, real-world primes  $p$  are large and computing  $x^{p-2}$  by repeated multiplication of  $x$  with itself is infeasible. A “double and multiply” approach (as described in XXX) is faster, as it computes the power in roughly  $\log_2(p)$  steps, but still adds a lot of constraints to the circuit.

Computing inverses in the circuit makes no use of the fact that inversion is a native operation in any field. A more constraints friendly approach is therefore to compute the multiplicative inverse outside of the circuit and then only enforce correctness of the computation in the circuit.

To understand how this can be achieved, observe that a field element  $y \in \mathbb{F}$  is the multiplicative inverse of a field element  $x \in \mathbb{F}$  if and only if  $x \cdot y = 1$  in  $\mathbb{F}$ . We can use this, and define a circuit that has two inputs,  $x$  and  $y$ , and enforces  $x \cdot y = 1$ . It is then guaranteed that  $y$  is the multiplicative inverse of  $x$ . The price we pay is that we can not compute  $y$  by circuit execution, but auxiliary data is needed to tell any prover which value of  $y$  is needed for a valid circuit assignment. The following circuit defines the constraint



Using the general method from 6.2.1.1, the circuit is transformed into the following rank-1 constraint system:

$$S_1 \cdot S_2 = 1 \quad (7.4)$$

Any valid assignment  $\{S_1, S_2\}$  to this circuit enforces that  $S_2$  is the multiplicative inverse of  $S_1$ , and, since there is no field element  $S_2$  such that  $0 \cdot S_2 = 1$ , it also handles the fact that the multiplicative inverse of 0 is not defined in any field.

Real-world compilers usually provide a gadget or a function to abstract over this circuit, and those functions compute the inverse  $x^{-1}$  as part of their witness generation process. Programmers then don’t have to care about providing the inverse as auxiliary data to the circuit. In PAPER, we define the following inversion function that compiles to the previous circuit:

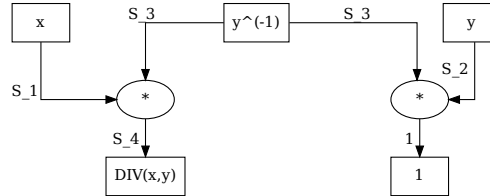
```
fn INV(x : F, y : F) -> (x_inv : F) {
  constant c : F = 1 ;
  c <== MUL( x , y ) ;
  x_inv <== y ;
}
```

As we see, this functions takes two inputs, the field value and its inverse. It therefore does not handle the computation of the inverse by itself. This is to keep PAPER as simple as possible.

In the setup phase, we compile every occurrence of the INV function into an instance of the inversion circuit XXX, and edge labels are generated according to the rules from XXX.

**The Division Constraint System** By definition, algebraic circuits only contain addition and multiplication gates, and it follows that there is no single gate for field division, despite the fact that division is a native operation in every field.

Implementing division as a circuit, we use the fact that division is multiplication with the multiplicative inverse. We therefore define division as a circuit using the inversion circuit and constraint system from the previous paragraph. Expensive inversion is computed outside of the circuit and then provided as circuit input. We get



Using the method from 6.2.1.1, we transform this circuit into the following rank-1 constraint system:

$$\begin{aligned} S_2 \cdot S_3 &= 1 \\ S_1 \cdot S_3 &= S_4 \end{aligned}$$

Any valid assignment  $\{S_1, S_2, S_3, S_4\}$  to this circuit enforces  $S_4$  to be the field division of  $S_1$  by  $S_2$ . It handles the fact that division by 0 is not defined, since there is no valid assignment in case  $S_2 = 0$ .

In PAPER, we define the following division function that compiles to the previous circuit:

```
fn DIV(x : F, y : F, y_inv : F) -> (DIV : F) {
  DIV <== MUL( x , INV( y, y_inv ) ) ;
}
```

In the setup phase, we compile every occurrence of the binary INV operator into an instance of the inversion circuit.

**Exercise 56.** Let  $F$  be the field  $\mathbb{F}_5$  of modular 5 arithmetics from example 14. Brain-compile the following PAPER statement into an algebraic circuit:

```
statement STUPID_CIRC {F: F_5} {
  fn foo(in_1 : F, in_2 : F)->(out_1 : F, out_2 : F){
    constant c_1 : F = 3 ;
    out_1<== ADD( MUL( c_1 , in_1 ) , in_1 ) ;
    out_2<== INV( c_1 , in_2 ) ;
  } ;

  fn main(in_1 : F, in_2 : F)->(out_1 : F, out_2 : TYPE_2){
    constant (c_1,c_2) : (F,F) = (3,2) ;
    (out_1,out_2) <== foo(in_1, in_2) ;
  } ;
}
```

**Exercise 57.** Consider the tiny-jubjub curve from example 69 and its associated circuit 128. Write a statement in PAPER that brain-compiles the statement into a circuit equivalent to the one derived in XXX, assuming that curve points are instances and every other assignment is a witness.



5258 *Exercise 58.* Let  $F = \mathbb{F}_{13}$  be the modular 13 prime field and  $x \in F$  some field element. Define a  
 5259 statement in PAPER such that given instance  $x$  a field element  $y \in F$  is a witness for the statement  
 5260 if and only if  $y$  is the square root of  $x$ .

5261 Brain-compile the statement into a circuit and derive its associated rank-1 constraint system.  
 5262 Consider the instance  $x = 9$  and compute a constructive proof for the statement.

### 5263 The boolean Type

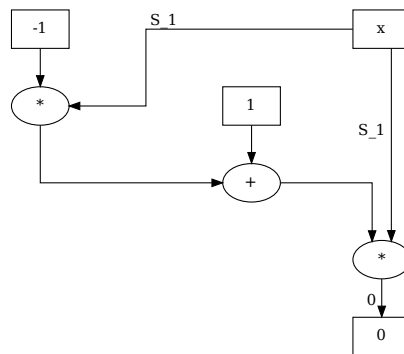
5264 Booleans are a classical primitive type, implemented by virtually every higher programing lan-  
 5265 guage. It is therefore important to implement booleans in circuits. One of the most common  
 5266 ways to do this is by interpreting the additive and multiplicative neutral element  $\{0, 1\} \subset \mathbb{F}$  as  
 5267 the two boolean values such that 0 represents *false* and 1 represents *true*. boolean operators  
 5268 like *and*, *or*, or *xor* are then expressible as algebraic computations inside  $\mathbb{F}$ .

5269 Representing booleans this way is convenient, because the elements 0 and 1 are defined in  
 5270 any field. The representation is therefore independent of the actual field in consideration.

5271 To fix boolean algebra notation, we write 0 to represent *false* and 1 to represent *true*, and  
 5272 we write  $\wedge$  to represent the boolean AND as well as  $\vee$  to represent the boolean OR operator.  
 5273 The boolean NOT operator is written as  $\neg$ .

5274 **The boolean Constraint System** To represent booleans by the additive and multiplicative  
 5275 neutral elements of a field, a constraint is required to actually enforce variables of boolean type  
 5276 to be either 1 or 0. In fact, many of the following circuits that represent boolean functions are  
 5277 only correct under the assumption that their input variables are constrained to be either 0 or 1.  
 5278 Not constraining boolean variables is a common problem in circuit design.

5279 In order to constrain an arbitrary field element  $x \in \mathbb{F}$  to be 1 or 0, the key observation is  
 5280 that the equation  $x \cdot (1 - x) = 0$  has only two solutions 0 and 1 in any field. Implementing this  
 5281 equation as a circuit therefore generates the correct constraint:



5282

Using the method from 6.2.1.1, we transform this circuit into the following rank-1 constraint system:

$$S_1 \cdot (1 - S_1) = 0$$

check  
reference

5283 Any valid assignment  $\{S_1\}$  to this circuit enforces  $S_1$  to be either 0 or 1.

5284 Some real-world circuit compilers (like ZOKRATES or BELLMAN) are typed, while others  
 5285 (like circom) are not. However, all of them have their way of dealing with the binary con-  
 5286 straint. In PAPER, we define the following boolean type that compiles to the previous circuit:

```

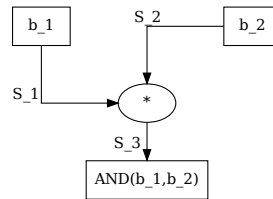
5287 type BOOL(b : BOOL) -> (x : F) {
5288     constant c1 : F = 0 ;
5289     constant c2 : F = 1 ;
5290     constant c3 : F = -1 ;
5291     c1 <== MUL( x , ADD( c2 , MUL( x , c3 ) ) ) ;
5292     x <== b ;
5293 }

```

5294 In the setup phase of a statement, we compile every occurrence of a variable of boolean type  
5295 into an instance of its associated boolean circuit.

5296 **The AND operator constraint system** Given two field elements  $b_1$  and  $b_2$  from  $\mathbb{F}$  that are  
5297 constrained to represent boolean variables, we want to find a circuit that computes the logical  
5298 **and** operator  $AND(b_1, b_2)$  as well as its associated R1CS that enforces  $b_1, b_2, AND(b_1, b_2)$  to  
5299 satisfy the constraint system if and only if  $b_1 \wedge b_2 = AND(b_1, b_2)$  holds true.

5300 The key insight here is that, given three boolean constraint variables  $b_1, b_2$  and  $b_3$ , the  
5301 equation  $b_1 \cdot b_2 = b_3$  is satisfied in  $\mathbb{F}$  if and only if the equation  $b_1 \wedge b_2 = b_3$  is satisfied in  
5302 boolean algebra. The logical operator  $\wedge$  is therefore implementable in  $\mathbb{F}$  by field multiplication  
5303 of its arguments and the following circuit computes the  $\wedge$  operator in  $\mathbb{F}$ , assuming all inputs are  
5304 restricted to be 0 or 1:



5305

5306 The associated rank-1 constraint system can be deduced from the general process 6.2.1.1 and  
5307 consists of the following constraint:

$$S_1 \cdot S_2 = S_3 \quad (7.5)$$

check  
reference

5308 Common circuit languages typically provide a gadget or a function to abstract over this circuit  
5309 such that programers can use the  $\wedge$  operator without caring about the associated circuit. In  
5310 PAPER, we define the following function that compiles to the  $\wedge$ -operator's circuit:

```

5311 fn AND(b_1 : BOOL, b_2 : BOOL) -> AND(b_1, b_2) : BOOL{
5312     AND(b_1, b_2) <== MUL( b_1 , b_2 ) ;
5313 }

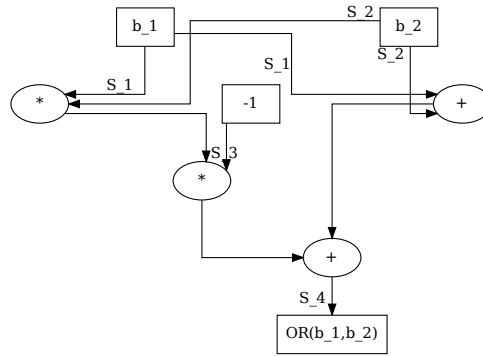
```

5314 In the setup phase of a statement, we compile every occurrence of the AND function into an  
5315 instance of its associated  $\wedge$ -operator's circuit.

5316 **The OR operator constraint system** Given two field elements  $b_1$  and  $b_2$  from  $\mathbb{F}$  that are  
5317 constrained to represent boolean variables, we want to find a circuit that computes the logical  
5318 **or** operator  $OR(b_1, b_2)$  as well as its associated R1CS that enforces  $b_1, b_2, OR(b_1, b_2)$  to satisfy  
5319 the constraint system if and only if  $b_1 \vee b_2 = OR(b_1, b_2)$  holds true.

5320 Assuming that three variables  $b_1, b_2$  and  $b_3$  are boolean constraint, the equation  $b_1 + b_2 - b_1 \cdot$   
5321  $b_2 = b_3$  is satisfied in  $\mathbb{F}$  if and only if the equation  $b_1 \vee b_2 = b_3$  is satisfied in boolean algebra.  
5322 The logical operator  $\vee$  is therefore implementable in  $\mathbb{F}$  by the following circuit, assuming all  
5323 inputs are restricted to be 0 or 1:

"constraints"  
or "con-  
strained"?



5324

The associated rank-1 constraint system can be deduced from the general process 6.2.1.1 and consists of the following constraints:

check  
reference

$$\begin{aligned} S_1 \cdot S_2 &= S_3 \\ (S_1 + S_2 - S_3) \cdot 1 &= S_4 \end{aligned}$$

5325 Common circuit languages typically provide a gadget or a function to abstract over this circuit  
5326 such that programers can use the  $\vee$  operator without caring about the associated circuit. In  
5327 PAPER, we define the following function that compiles to the  $\vee$ -operator's circuit:

```
5328 fn OR(b_1 : BOOL, b_2 : BOOL) -> OR(b_1, b_2) : BOOL{
5329   constant c1 : F = -1 ;
5330   OR(b_1, b_2) <== ADD(ADD(b_1, b_2), MUL(c1, MUL(b_1, b_2))) ;
5331 }
```

5332 In the setup phase of a statement, we compile every occurrence of the OR function into an  
5333 instance of its associated  $\vee$ -operator's circuit.

5334 *Exercise 59.* Let  $\mathbb{F}$  be a finite field and let  $b_1$  as well as  $b_2$  two boolean constraint variables from  
5335  $\mathbb{F}$ . Show that the equation  $OR(b_1, b_2) = 1 - (1 - b_1) \cdot (1 - b_2)$  holds true.

5336 Use this equation to derive an algebraic circuit with ingoing variables  $b_1$  and  $b_2$  and out-  
5337 going variable  $OR(b_1, b_2)$  such that  $b_1$  and  $b_2$  are boolean **constraint** and the circuit has a valid  
5338 assignment, if and only if  $OR(b_1, b_2) = b_1 \vee b_2$ .

"constraints"  
or "con-  
strained"?

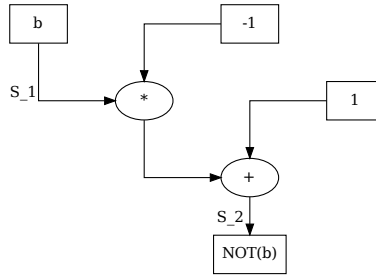
5339 Use the technique from XXX to transform this circuit into a rank-1 constraint system and  
5340 find its full solution set. Define a PAPER function that brain-compiles into the circuit.

add refer-  
ence

5341 **The NOT operator constraint system** Given a field element  $b$  from  $\mathbb{F}$  that is constrained to  
5342 represent a boolean variable, we want to find a circuit that computes the logical **NOT** operator  
5343  $NOT(b)$  as well as its associated RICS that enforces  $b, NOT(b)$  to satisfy the constraint system  
5344 if and only if  $\neg b = NOT(b)$  holds true.

5345 Assuming that two variables  $b_1$  and  $b_2$  are boolean **constraint**, the equation  $(1 - b_1) = b_2$  is  
5346 satisfied in  $\mathbb{F}$  if and only if the equation  $\neg b_1 = b_2$  is satisfied in boolean algebra. The logical  
5347 operator  $\neg$  is therefore implementable in  $\mathbb{F}$  by the following circuit, assuming all inputs are  
5348 restricted to be 0 or 1:

"constraints"  
or "con-  
strained"?



5349

The associated rank-1 constraint system can be deduced from the general process XXX and consists of the following constraints

add reference

$$(1 - S_1) \cdot 1 = S_2$$

5350 Common circuit languages typically provide a gadget or a function to abstract over this circuit  
 5351 such that programers can use the  $\neg$  operator without caring about the associated circuit. In  
 5352 PAPER, we define the following function that compiles to the  $\neg$ -operator's circuit:

```

5353 fn NOT(b : BOOL -> NOT(b) : BOOL{
5354   constant c1 = 1 ;
5355   constant c2 = -1 ;
5356   NOT(b_1) <== ADD( c1 , MUL( c2 , b ) ) ;
5357 }
```

5358 In the setup phase of a statement, we compile every occurrence of the NOT function into an  
 5359 instance of its associated  $\neg$ -operator's circuit.

5360 *Exercise 60.* Let  $\mathbb{F}$  be a finite field. Derive the algebraic circuit and associated rank-1 constraint  
 5361 system for the following operators: NOR, XOR, NAND, EQU.

5362 **Modularity** As we have seen in chapter 6,, both algebraic circuits and R1CS have a modular-  
 5363 ity property, and as we have seen in this section, all basic boolean functions are expressible in  
 5364 circuits. Combining those two properties, show that it is possible to express arbitrary boolean  
 5365 functions as algebraic circuits.

check references

5366 This shows that the expressiveness of algebraic circuits and therefore rank-1 constraint sys-  
 5367 tems is as general as the expressiveness of boolean circuits. An important implication is that  
 5368 the languages  $L_{R1CS-SAT}$  and  $L_{Circuit-SAT}$  as defined in 4, are as general as the famous language  
 5369  $L_{3-SAT}$ , which is known to be  $\mathcal{NP}$ -complete.

check reference

5370 *Example 132.* To give an example of how a compiler might construct complex boolean expres-  
 5371 sions in algebraic circuits from simple ones and how we derive their associated rank-1 constraint  
 5372 systems, let's look at the following PAPER statement:

```

5373 statement BOOLEAN_STAT {F: F_p} {
5374   fn main(b_1:BOOL,b_2:BOOL,b_3:BOOL,b_4:BOOL )-> pub b_5:BOOL {
5375     b_5 <== AND( OR( b_1 , b_2 ) , AND( b_3 , NOT( b_4 ) ) ) ;
5376   } ;
5377 }
```

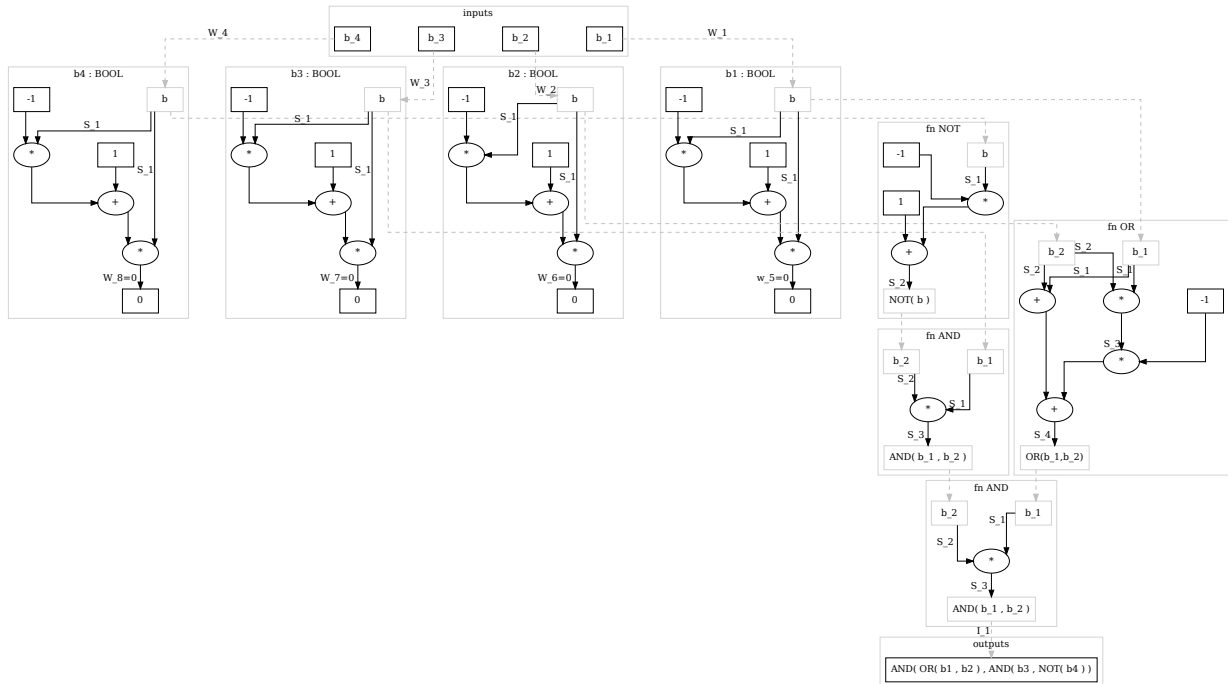
The code describes a circuit that takes four private inputs  $b_1, b_2, b_3$  and  $b_4$  of boolean type and computes a public output  $b_5$  such that the following boolean expression holds true:

$$(b_1 \vee b_2) \wedge (b_3 \wedge \neg b_4) = b_5$$

During a setup-phase, a circuit compiler transforms this high-level language statement into a circuit and associated rank-1 constraint systems and hence defines a language  $L_{BOOLEAN\_STAT}$ .

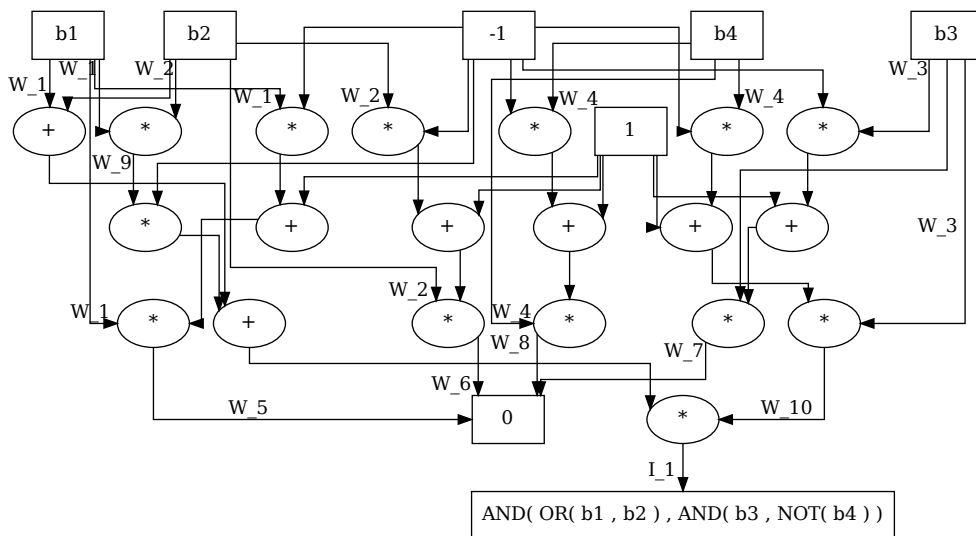
To see how this might be achieved, we use PAPER as an example to execute the setup-phase and compile `BOOLEAN_STAT` into a circuit. Taking the definition of the boolean constraint `XXX` as well as the definitions of the appropriate boolean operators into account, we get the following circuit:

add reference



Simple optimization then collapses all box-nodes that are directly linked and all box nodes that represent the same constants. After relabeling the edges, the following circuit represents the circuit associated to the `BOOLEAN_STAT` statement:

can we rotate this by 90°?



5392 Given some public input  $I_1$  from  $\mathbb{F}_{13}$ , a valid assignment to this circuit consists of private inputs  
 5393  $W_1, W_2, W_3, W_4$  from  $\mathbb{F}_{13}$  such that the equation  $I_1 = (W_1 \vee W_2) \wedge (W_3 \wedge \neg W_4)$  holds true. In  
 5394 addition, a valid assignment also has to contain private inputs  $W_5, W_6, W_7, W_8, W_9$  and  $W_{10}$ ,  
 5395 which can be derived from circuit execution. The inputs  $W_5, \dots, W_8$  ensure that the first four  
 5396 private inputs are either 0 or 1 but not any other field element, and the others enforce the boolean  
 5397 operations in the expression.

To compute the associated R1CS, we can use the general method from 6.2.1.1 and look at every labeled outgoing edge not coming from a source node. We declare the edges coming from input nodes as well as the edge going to the single output node as public, and every other edge as private input. In this case we get:

check  
reference

$$\begin{aligned}
 W_5 : W_1 \cdot (1 - W_1) &= 0 && \text{boolean constraints} \\
 W_6 : W_2 \cdot (1 - W_2) &= 0 \\
 W_7 : W_3 \cdot (1 - W_3) &= 0 \\
 W_8 : W_4 \cdot (1 - W_4) &= 0 \\
 W_9 : W_1 \cdot W_2 &= W_9 && \text{first OR-operator constraint} \\
 W_{10} : W_3 \cdot (1 - W_4) &= W_{10} && \text{AND(.,NOT(.))-operator constraints} \\
 I_1 : (W_1 + W_2 - W_9) \cdot W_{10} &= I_1 && \text{AND-operator constraints}
 \end{aligned}$$

5398 The reason why this R1CS only contains a single constraint for the multiplication gate in the  
 5399 OR-circuit, while the general definition XXX requires two constraints, is that the second con-  
 5400 straint in XXX only appears because the final addition gate is connected to an output node. In  
 5401 this case, however, the final addition gate from the OR-circuit is enforced in the left factor of  
 5402 the  $I_1$  constraint. Something similar holds true for the negation circuit.

add refer-  
ence

add refer-  
ence

During a prover-phase, some public instance  $I_5$  must be given. To compute a constructive proof for the statement of the associated languages with respect to instance  $I_5$ , a prover has to find four boolean values  $W_1, W_2, W_3$  and  $W_4$  such that

$$(W_1 \vee W_2) \wedge (W_3 \wedge \neg W_4) = I_5$$

5403 holds true. In our case neither the circuit nor the PAPER statement specifies how to find those  
 5404 values, and it is a problem that any prover has to solve outside of the circuit. This might or  
 5405 might not be true for other problems, too. In any case, once the prover found those values, they  
 5406 can execute the circuit to find a valid assignment.

To give a concrete example, let  $I_1 = 1$  and assume  $W_1 = 1, W_2 = 0, W_3 = 1$  and  $W_4 = 0$ . Since  $(1 \vee 0) \wedge (1 \wedge \neg 0) = 1$ , those values satisfy the problem and we can use them to execute the circuit. We get

$$\begin{aligned}
 W_5 &= W_1 \cdot (1 - W_1) = 0 \\
 W_6 &= W_2 \cdot (1 - W_2) = 0 \\
 W_7 &= W_3 \cdot (1 - W_3) = 0 \\
 W_8 &= W_4 \cdot (1 - W_4) = 0 \\
 W_9 &= W_1 \cdot W_2 = 0 \\
 W_{10} &= W_3 \cdot (1 - W_4) = 1 \\
 I_1 &= (W_1 + W_2 - W_9) \cdot W_{10} = 1
 \end{aligned}$$

5407 A constructive proof of knowledge of a witness, for instance,  $I_1 = 1$ , is therefore given by the  
 5408 tuple  $P = (W_5, W_6, W_7, W_8, W_9, W_{10}) = (0, 0, 0, 0, 0, 1)$ .

## Arrays

The `array` type represents a fixed-size collection of elements of equal type, each selectable by one or more indices that can be computed at run time during program execution.

Arrays are a classical type, implemented by many higher programming languages that compile to circuits or rank-1 constraint systems. However, most high-level circuit languages support **static** arrays, i.e., arrays whose length is known at compile time only.

The most common way to compile arrays to circuits is to transform any array of a given type  $\tau$  and size  $N$  into  $N$  circuit variables of type  $\tau$ . Arrays are therefore **syntactic sugar**, that is, parts of the formal language that makes the code easier for humans to read, which the compiler transforms into input nodes, much like any other variable. In PAPER, we define the following array type:

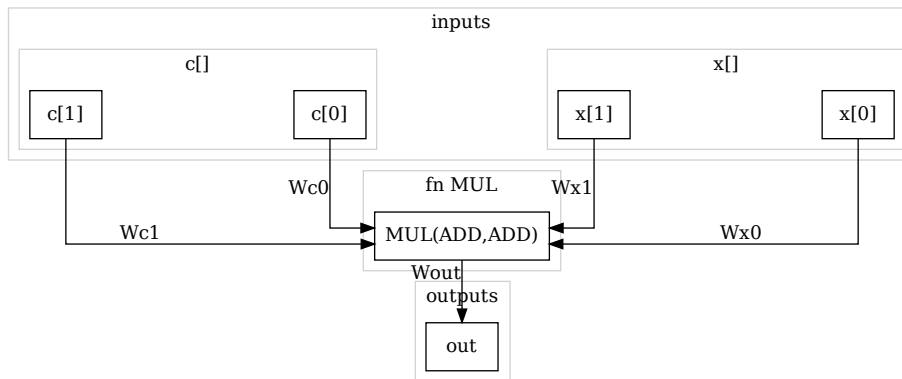
```
type <Name>: <Type>[N : unsigned] -> (Type,...) {
  return (<Name>[0],...)
}
```

In the setup phase of a statement, we compile every occurrence of an array of size  $N$  that contains elements of type `Type` into  $N$  variables of type `Type`.

*Example 133.* To give an intuition of how a real-world compiler might transform arrays into circuit variables, consider the following PAPER statement:

```
statement ARRAY_TYPE {F: F_5} {
  fn main(x: F[2]) -> F {
    let constant c: F[2] = [2,4] ;
    let out:F <== MUL(ADD(x[1],c[0]),ADD(x[0],c[1])) ;
    return out ;
  } ;
}
```

During a setup phase, a circuit compiler might then replace any occurrence of the array type by a tuple of variables of the underlying type, and then use those variables in the circuit synthesis process instead. To see how this can be achieved, we use PAPER as an example. Abstracting over the sub-circuit of the computation, we get the following circuit:



## The Unsigned Integer Type

Unsigned integers of size  $N$ , where  $N$  is usually a power of two, represent non-negative integers in the range  $0 \dots 2^N - 1$ . They have a notion of addition, subtraction and multiplication, defined

5442 by modular  $2^N$  arithmetics. If some  $N$  is given, we write  $\text{uN}$  for the associated type.

5443 **The  $\text{uN}$  Constraint System** Many high-level circuit languages define the the various  $\text{uN}$  types  
 5444 as arrays of size  $N$ , where each element is of boolean type. This is similar to their representa-  
 5445 tion on common computer hardware and allows for efficient and straightforward definition of  
 5446 common operators, like the various **shift**, or logical operators.

shift

5447 If some unsigned integer  $N$  is known at compile time in PAPER, we define the following  $\text{uN}$   
 5448 type:

```
5449 type uN -> BOOL[N] {
5450   let base2 : BOOL[N] <== BASE_2 (uN) ;
5451   return base2 ;
5452 }
```

To enforce an  $N$ -tuple of field elements  $(b_0, \dots, b_{N-1})$  to represent an element of type  $\text{uN}$  we therefore need  $N$  boolean constraints

$$\begin{aligned} S_0 \cdot (1 - S_0) &= 0 \\ S_1 \cdot (1 - S_1) &= 0 \\ &\dots \\ S_{N-1} \cdot (1 - S_{N-1}) &= 0 \end{aligned}$$

5453 In the setup phase of a statement, we compile every occurrence of the  $\text{uN}$  type by a size  $N$  array  
 5454 of boolean type. During a=the prover phase, actual elements of the  $\text{uN}$  type are first transformed  
 5455 into binary representation and then this binary representation is assigned to the boolean array  
 5456 that represents the  $\text{uN}$  type.

5457 *Remark 6.* Representing the  $\text{uN}$  type as boolean arrays is conceptually clean and works over  
 5458 generic base fields. However, representing unsigned integers in this way requires a lot of space  
 5459 as every bit is represented as a field element and if the base field is large, those field elements  
 5460 require considerable space in hardware.

5461 It should be noted that, in some cases, there is another, more space- and constraint-efficient  
 5462 approach for representing unsigned integers that can be used whenever the underlying base field  
 5463 is sufficiently large. To understand this, recall that addition and multiplication in a prime field  
 5464  $\mathbb{F}_p$  is equal to addition and multiplication of integers, as long as the sum or the product does  
 5465 not exceed the modulus  $p$ . It is therefore possible to represent the  $\text{uN}$  type inside the base-field  
 5466 type whenever  $N$  is small enough. In this case, however, care has to be taken to never overflow  
 5467 the modulus. It is also important to make sure that, in the case of subtraction, the subtrahend is  
 5468 never larger than the minuend.

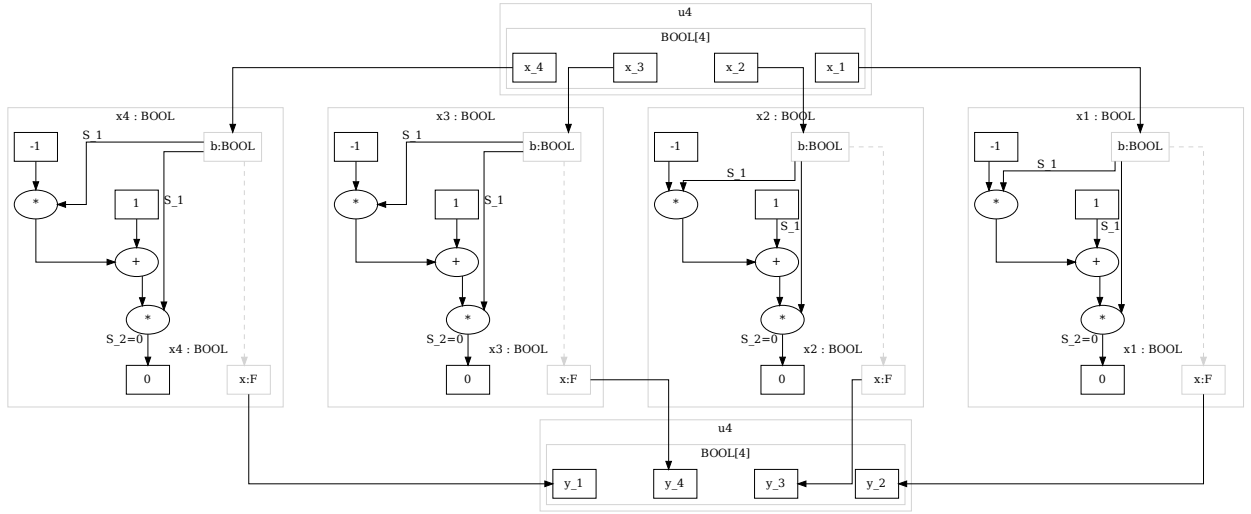
5469 *Example 134.* To give an intuition of how a real-world compiler might transform unsigned  
 5470 integers into circuit variables, consider the following PAPER statement:

```
5471 statement RING_SHIFT{F: F_p, N=4} {
5472   fn main(x: uN) -> uN {
5473     let y:uN <== [x[1], x[2], x[3], x[0]] ;
5474     return y ;
5475   } ;
5476 }
```

5477 During the setup-phase, a circuit compiler might then replace any occurrence of the  $\text{uN}$  type  
 5478 by  $N$  variables of `boolean` type. Using the definition of booleans, each of these variables is



then transformed into the `field` type and a boolean constraint system. To see how this can be achieved, we use PAPER as an example and get the following circuit:



During the prover phase, the function `main` is called with an actual input of `u4` type, say  $x=14$ . The high-level language then has to transform the decimal value 14 into its 4-bit binary representation  $14_2 = (0, 1, 1, 1)$  outside of the circuit. Then the array of field values  $x[4] = [0, 1, 1, 1]$  is used as an input to the circuit. Since all 4 field elements are either 0 or 1, the four boolean constraints are satisfiable and the output is an array of the four field elements  $[1, 1, 1, 0]$ , which represents the `u4` element 7.

**The Unigned Integer Operators** Since elements of `uN` type are represented as boolean arrays, shift operators are implemented in circuits simply by rewiring the boolean input variables to the output variables accordingly.

Logical operators, like AND, OR, or NOT are defined on the `uN` type by invoking the appropriate boolean operators bitwise to every bit in the boolean array that represents the `uN` element.

Addition and multiplication can be represented similarly to how machines represent those operations. Addition can be implemented by first defining the **full adder** circuit and then combining  $N$  of these circuits into a circuit that adds two elements from the `uN` type.

**Exercise 61.** Let  $F = \mathbb{F}_{13}$  and  $N=4$  be fixed. Define circuits and associated R1CS for the left and right **bishift** operators  $x \ll 2$  as well as  $x \gg 2$  that operate on the `uN` type. Execute the associated circuit for  $x : u4 = 11$ .

**Exercise 62.** Let  $F = \mathbb{F}_{13}$  and  $N=2$  be fixed. Define a circuit and associated R1CS for the addition operator  $\text{ADD} : F \times F \rightarrow F$ . Execute the associated circuit to compute  $\text{ADD}(2, 7)$ .

**Exercise 63.** Brain-compile the following PAPER code into a circuit and derive the associated R1CS.

```
statement MASK_MERGE {F:F_5, N=4} {
  fn main(pub a : uN, pub b : uN) -> F {
    let constant mask : uN = 10 ;
    let r : uN <== XOR(a, AND(XOR(a, b), mask)) ;
    return r ;
```

```

5510     }
5511 }

```

5512 Let  $L_{mask\_merge}$  be the language defined by the circuit. Provide a constructive knowledge proof  
 5513 in  $L_{mask\_merge}$  for the instance  $I = (I_a, I_b) = (14, 7)$ .

## 5514 7.2.2 Control Flow

5515 Most programing languages of the imperative or functional style have some notion of basic  
 5516 control structures to direct the order in which instructions are evaluated. Contemporary circuit  
 5517 compilers usually provide a single thread of execution and provide basic flow constructs that  
 5518 implement control flow in circuits.

### 5519 The Conditional Assignment

5520 Writing high-level code that compiles to circuits, it is often necessary to have a way for condi-  
 5521 tional assignment of values or computational output to variables.

5522 One way to realize this in many programming languages is in terms of the conditional  
 5523 ternary assignment operator  $?$ : that branches the control flow of a program according to some  
 5524 condition and then assigns the output of the computed branch to some variable.

```

5525 variable = condition ? value_if_true : value_if_false

```

5526 In this description, `condition` is a boolean expression and `value_if_true` as well as  
 5527 `value_if_false` are expressions that evaluate to the same type as `variable`.

5528 In programming languages like Rust, another way to write the conditional assignment oper-  
 5529 ator that is more familiar to many programmers is given by

```

5530 variable = if condition then {
5531     value_if_true
5532 } else {
5533     value_if_false
5534 }

```

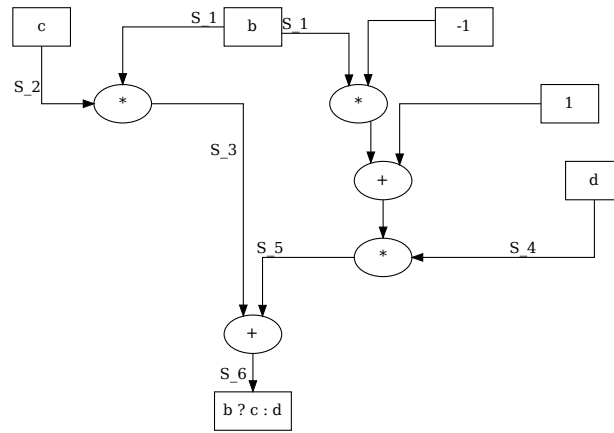
5535 In most programing languages, it is a key property of the ternary assignment operator that  
 5536 the expression `value_if_true` is only evaluated if `condition` evaluates to true and the  
 5537 expression `value_if_false` is only evaluated if `condition` evaluates to false. In fact,  
 5538 computer programs would turn out to be very inefficient if the ternary operator would evaluate  
 5539 both expressions regardless of the value of `condition`.

5540 A simple way to implement conditional assignment operator as a circuit can be achieved  
 5541 if the requirement that only one branch of the conditional operator is executed is dropped. To  
 5542 see that, let  $b$ ,  $c$  and  $d$  be field elements such that  $b$  is a boolean constraint. In this case, the  
 5543 following equation enforces a field element  $x$  to be the result of the conditional assignment  
 5544 operator:

$$x = b \cdot c + (1 - b) \cdot d \quad (7.6)$$

5545 Expressing this equation in terms of the addition and multiplication operators from XXX, we  
 5546 can flatten it into the following algebraic circuit:

add refer-  
ence



5547

5548 Note that, in order to compute a valid assignment to this circuit, both  $S_2$  as well as  $S_4$  are  
 5549 necessary. If the inputs to the nodes  $c$  and  $d$  are circuits themselves, both circuits need valid  
 5550 assignments and therefore have to be executed. As a consequence, this implementation of  
 5551 the conditional assignment operator has to execute all branches of all circuits, which is very  
 5552 different from the execution of common computer programs and contributes to the increased  
 5553 computational effort any prover has to invest, in contrast to the execution in other programming  
 5554 models.

We can use the general technique from 6.2.1.1 to derive the associated rank-1 constraint system of the conditional assignment operator. We get the following:

 check  
reference

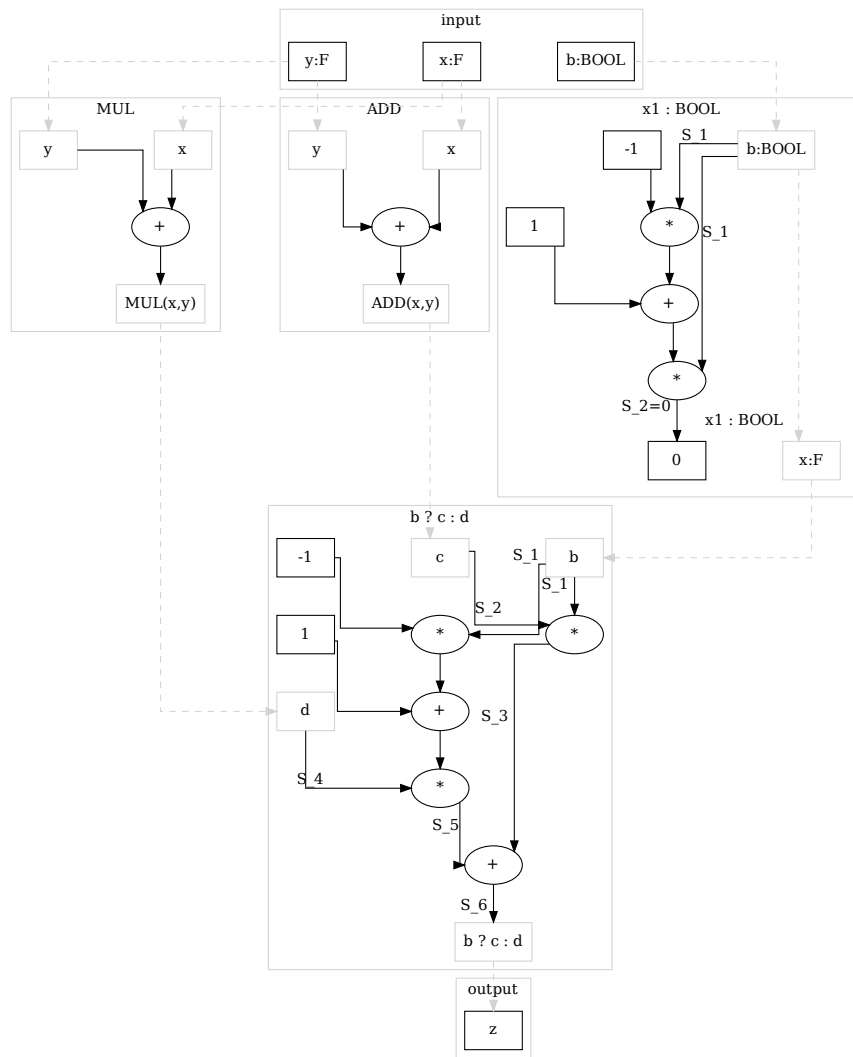
$$\begin{aligned} S_1 \cdot S_2 &= S_3 \\ (1 - S_1) \cdot S_4 &= S_5 \\ (S_3 + S_5) \cdot 1 &= S_6 \end{aligned}$$

5555 *Example 135.* To give an intuition of how a real-world circuit compiler might transform any  
 5556 high-level description of the conditional assignment operator into a circuit, consider the follow-  
 5557 ing PAPER code:

```

5558 statement CONDITIONAL_OP {F:F_p} {
5559   fn main(x : F, y : F, b : BOOL) -> F {
5560     let z : F <== if b then {
5561       ADD(x,y)
5562     } else {
5563       MUL(x,y)
5564     } ;
5565     return z ;
5566   }
5567 }
```

5568 Brain-compiling this code into a circuit, we first draw box nodes for all input and output vari-  
 5569 ables, and then transform the boolean type into the field type together with its associated con-  
 5570 straint. Then we evaluate the assignments to the output variables. Since the conditional assign-  
 5571 ment operator is the top level function, we draw its circuit and then draw the circuits for both  
 5572 conditional expressions. We get the following:



5573

5574 **Loops**

5575 In many programming languages, various loop control structures are defined that allow devel-  
 5576 opers to execute expressions with a specified number of repetitions or arguments. In particular,  
 5577 it is often possible to implement unbounded loops like the loop structure give below, where the  
 5578 number of executions depends on execution inputs and is therefore unknown at compile time:

5579 **while** true do { }  
 5580

5581 **M:** Add another example where the loop actually depends on the input.

 Add ex-  
ample

5582 In contrast to this, it should be noted that algebraic circuits and rank-1 constraint systems  
 5583 are not general enough to express arbitrary computation, but bounded computation only. As a  
 5584 consequence, it is not possible to implement unbounded loops, or loops with bounds that are  
 5585 unknown at compile time in those models. This can be easily seen since circuits are acyclic  
 5586 by definition, and implementing an unbounded loop as an acyclic graph requires a circuits of  
 5587 unbounded size.

5588 However, circuits are general enough to express bounded loops, where the upper bound on  
 5589 its execution is known at compile time. Those loop can be implemented in circuits by enrolling  
 5590 the loop.

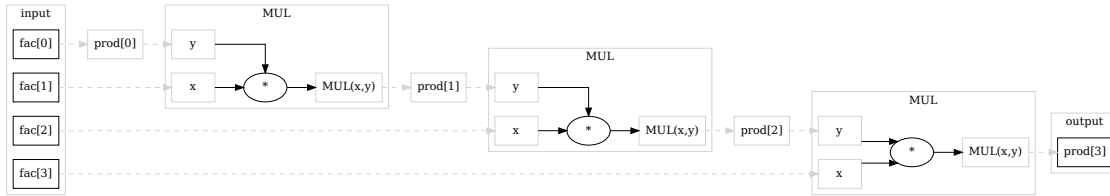
As a consequence, any programming language that compiles to algebraic circuits can only provide loop structures where the bound is a constant known at compile time. This implies that loops cannot depend on execution inputs, but on compile time parameters only.

*Example 136.* To give an intuition of how a real-world circuit compiler might transform any high-level description of a bounded `for` loop into a circuit, consider the following PAPER code:

```
statement FOR_LOOP {F:F_p, N: unsigned = 4} {
  fn main(fac : F[N]) -> F {
    let prod[N] : F ;
    prod[0] <== fac[0] ;
    for unsigned i in 1..N do [{
      prod[i] <== MUL(fac[i], prod[i-1]) ;
    }]
    return prod[N] ;
  }
}
```

Note that, in a program like this, the loop counter `i` has no expression in the derived circuit. It is pure syntactic sugar, telling the compiler how to unroll the loop.

Brain-compiling this code into a circuit, we first draw box nodes for all input and output variables, noting that the loop counter is not represented in the circuit. Since all variables are of `field` type, we don't have to compile any type constraints. Then we evaluate the assignments to the output variables by unrolling the loop into 3 individual assignment operators. We get:



### 7.2.3 Binary Field Representations

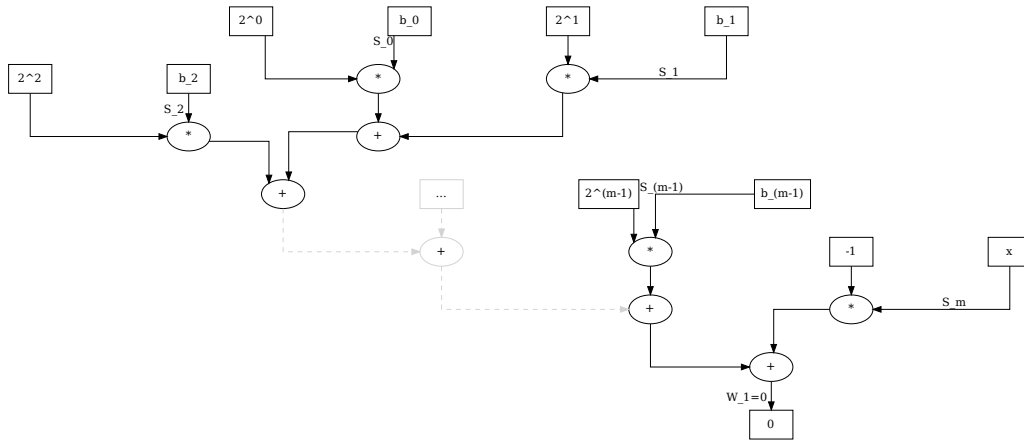
In applications, it is often necessary to enforce a binary representation of elements from the `field` type. To derive an appropriate circuit over a prime field  $\mathbb{F}_p$ , let  $m = \lceil \log_2 p \rceil$  be the smallest number of bits necessary to represent the prime modulus  $p$ . Then a bitstring  $(b_0, \dots, b_{m-1}) \in \{0, 1\}^m$  is a binary representation of a field element  $x \in \mathbb{F}_p$ , if and only if

$$x = b_0 \cdot 2^0 + b_1 \cdot 2^1 + \dots + b_{m-1} \cdot 2^{m-1}$$

In this expression, addition and exponentiation is considered to be executed in  $\mathbb{F}_p$ , which is well defined since all terms  $2^j$  for  $0 \leq j < m$  are elements of  $\mathbb{F}_p$ . Note, however, that in contrast to the binary representation of unsigned integers  $n \in \mathbb{N}$ , this representation is not unique in general, since the modular  $p$  equivalence class might contain more than one binary representative.

Considering that the underlying prime field is fixed and the most significant bit of the prime modulus is  $m$ , the following circuit flattens equation XXX, assuming all inputs  $b_1, \dots, b_m$  are of boolean type.

add reference



5622

Applying the general transformation rule to compute the associated rank-1 constraint systems, we see that we actually only need a single constraint to enforce some binary representation of any field element. We get

$$(S_0 \cdot 2^0 + S_1 \cdot 2^1 + \dots + S_{m-1} \cdot 2^{m-1} - S_m) \cdot 1 = 0$$

5623 Given an array `BOOL[N]` of  $N$  boolean constraint field elements and another field element  $x$ ,  
 5624 the circuit enforces `BOOL[N]` to be one of the binary representations of  $x$ . If `BOOL[N]` is not  
 5625 a binary representation of  $x$ , no valid assignment and hence no solution to the associated R1CS  
 5626 can exist.

5627 *Example 137.* Consider the prime field  $\mathbb{F}_{13}$ . To compute binary representations of elements  
 5628 from that field, we start with the binary representation of the prime modulus 13, which is  $|13|_2 =$   
 5629  $(1, 0, 1, 1)$  since  $13 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3$ . So  $m = 4$  and we need up to 4 bits to represent  
 5630 any element  $x \in \mathbb{F}_{13}$ .

To see that binary representations are not unique in general, consider the element  $2 \in \mathbb{F}_{13}$ . It has the binary representations  $|2|_2 = (0, 1, 0, 0)$  and  $|2|_2 = (1, 1, 1, 1)$ , since in  $\mathbb{F}_{13}$  we have

$$2 = \begin{cases} 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 \\ 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 \end{cases}$$

5631 This is because the unsigned integers 2 and 15 are both in the modular 13 remainder class of 2  
 5632 and hence are both representatives of 2 in  $\mathbb{F}_{13}$ .

To see how circuit XXX works, we want to enforce the binary representation of  $7 \in \mathbb{F}_{13}$ . Since  $m = 4$  we have to enforce a 4-bit representation for 7, which is  $(1, 1, 1, 0)$ , since  $7 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3$ . A valid circuit assignment is therefore given by  $(S_0, S_1, S_2, S_3, S_4) = (1, 1, 1, 0, 7)$  and, indeed, the assignment satisfies the required 5 constraints including the 4 boolean constraints for  $S_0, \dots, S_3$ :

$$\begin{aligned} 1 \cdot (1 - 1) &= 0 & // \text{boolean constraints} \\ 1 \cdot (1 - 1) &= 0 \\ 1 \cdot (1 - 1) &= 0 \\ 0 \cdot (1 - 0) &= 0 \\ (1 + 2 + 4 + 0 - 7) \cdot 1 &= 0 & // \text{binary rep. constraint} \end{aligned}$$

 add refer-  
ence

## 7.2.4 Cryptographic Primitives

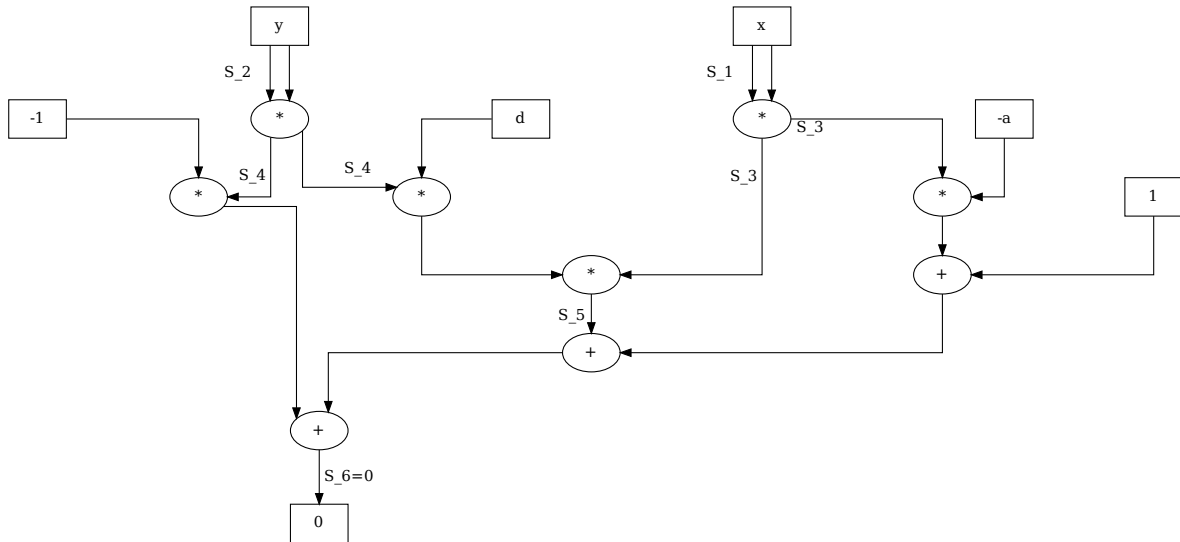
In applications, it is often required to do cryptography in a circuit. To do this, basic cryptographic primitives like hash functions or elliptic curve cryptography needs to be implemented as circuits. In this section, we give a few basic examples of how to implement such primitives.

### Twisted Edwards curves

Implementing elliptic curve cryptography in circuits means to implement the field equation as well as the algebraic operations of an elliptic curve as circuits. To do this efficiently, the curve must be defined over the same base field as the field that is used in the circuit.

For efficiency reasons, it is advantageous to choose an elliptic curve such that that all required constraints and operations can be implement with as few gates as possible. Twisted Edwards curves are particularly useful for that matter, since their addition law is particularly simple and the same equation can be used for all curve points including the point at infinity. This simplifies the circuit a lot.

**Twisted Edwards curve constraints** As we have seen in section 5.1.3, a twisted Edwards curve over a finite field  $F$  is defined as the set of all pairs of points  $(x, y) \in \mathbb{F} \times \mathbb{F}$  such that  $x$  and  $y$  satisfy the equation  $a \cdot x^2 + y^2 = 1 + d \cdot x^2 y^2$ . As we have seen in example XXX, we can transform this equation into the following circuit:



The circuit enforces the two inputs of `field` type to satisfy the twisted Edwards curve equation and, as we know from example XXX, the associated rank-1 constraint system is given by:

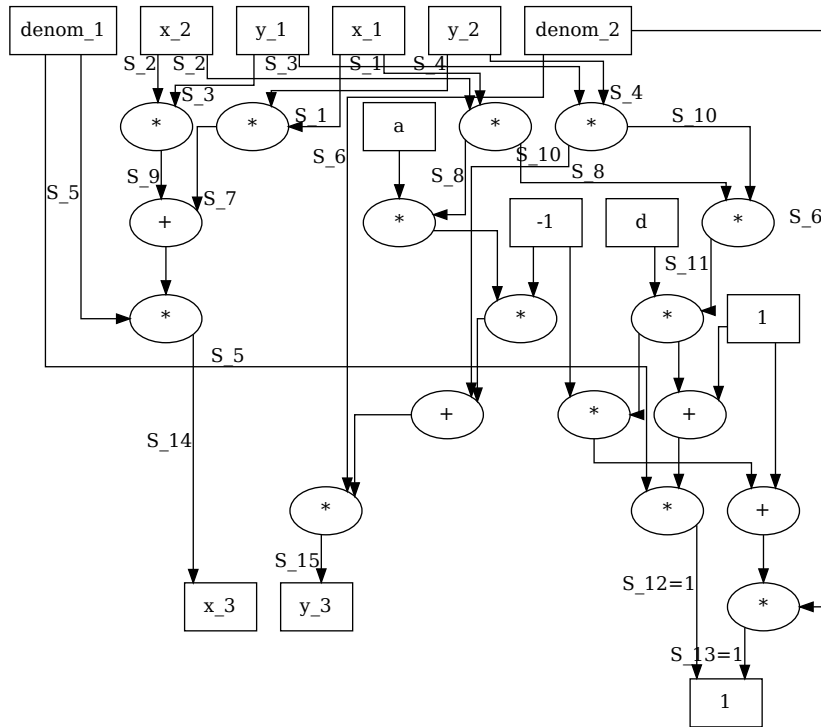
$$\begin{aligned}
 S_1 \cdot S_1 &= S_3 \\
 S_2 \cdot S_2 &= S_4 \\
 (S_4 \cdot 8) \cdot S_3 &= S_5 \\
 (12 \cdot S_4 + S_5 + 10 \cdot S_3 + 1) \cdot 1 &= 0
 \end{aligned}$$

**Exercise 64.** Write the circuit and associated rank-1 constraint system for a Weierstraß curve of a given field  $\mathbb{F}$ .

**Twisted Edwards curve addition** As we have seen in 5.1.3, a major advantage of twisted Edwards curves is the existence of an addition law that contains no branching and is valid for all curve points. Moreover, the neutral element is not “at infinity” but the actual curve point  $(0, 1)$ . In fact, given two points  $(x_1, y_1)$  and  $(x_2, y_2)$  on a twisted Edwards curve, their sum is defined as

$$(x_3, y_3) = \left( \frac{x_1 y_2 + y_1 x_2}{1 + d \cdot x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a \cdot x_1 x_2}{1 - d \cdot x_1 x_2 y_1 y_2} \right)$$

We can use the division circuit from XXX to flatten this equation into an algebraic circuit. Inputs to the circuit are then not only the two curve points  $(x_1, y_1)$  and  $(x_2, y_2)$ , but also the two denominators  $denum_1 = 1 + d \cdot x_1 x_2 y_1 y_2$  as well as  $denum_2 = 1 - d \cdot x_1 x_2 y_1 y_2$ , which any prover needs to compute outside of the circuit. We get



Using the general technique from XXX to derive the associated rank-1 constraint system, we get the following result:

$$\begin{aligned} S_1 \cdot S_4 &= S_7 \\ S_1 \cdot S_2 &= S_8 \\ S_2 \cdot S_3 &= S_9 \\ S_3 \cdot S_4 &= S_{10} \\ S_8 \cdot S_{10} &= S_{11} \\ S_5 \cdot (1 + d \cdot S_{11}) &= 1 \\ S_6 \cdot (1 - d \cdot S_{11}) &= 1 \\ S_5 \cdot (S_9 + S_7) &= S_{14} \\ S_6 \cdot (S_{10} - a \cdot S_8) &= S_{15} \end{aligned}$$



5660 *Exercise 65.* Let  $\mathbb{F}$  be a field. Define a circuit that enforces field inversion for a point of a  
5661 twisted Edwards curve over  $\mathbb{F}$ .

## Chapter 8

# Zero Knowledge Protocols

A so-called **zero-knowledge protocol** is a set of mathematical rules by which one party (usually called **the prover**) can convince another party (usually called **the verifier**) that a given statement is true, while not revealing any additional information apart from the truth of the statement.

As we have seen in chapter 6, given some language  $L$  and instance  $I$ , the knowledge claim “there is a witness  $W$  such that  $(I; W)$  is a word in  $L$ ” is constructively provable by providing  $W$  to the verifier. However, the challenge for a zero-knowledge protocol is to prove knowledge of a witness without revealing any information beyond its bare existence.

In this chapter, we look at various systems that exist to solve this task. We start with an introduction to the basic concepts and terminology in zero-knowledge proving systems and then introduce the so-called Groth\_16 protocol as one of the most efficient systems. We plan to update this chapter with new inventions in future versions of this book.

add reference

## 8.1 Proof Systems

From an abstract point of view, a proof system is a set of rules which models the generation and exchange of messages between two parties: a prover and a verifier. Its task is to ascertain whether a given string belongs to a formal language or not.

Proof systems are often classified by certain trust assumptions and the computational capabilities of both parties. In its most general form, the prover usually possesses unlimited computational resources but cannot be trusted, while the verifier has bounded computation power but is assumed to be honest.

Proving the membership statement for some string is executed by the generation of certain messages that are sent between prover and verifier, until the verifier is convinced that the string is an element of the language in consideration.

To be more specific, let  $\Sigma$  be an alphabet, and let  $L$  be a formal language defined over  $\Sigma$ . Then a **proof system** for language  $L$  is a pair of probabilistic interactive algorithms  $(P, V)$ , where  $P$  is called the **prover** and  $V$  is called the **verifier**.

Both algorithms are able to send messages to one another, and each algorithm has its own state, some shared initial state and access to the messages. The verifier is bounded to a number of steps which is polynomial in the size of the shared initial state, after which it stops and outputs either `accept` or `reject` indicating that it accepts or rejects a given string to be in  $L$ . In contrast, there are bounds on the computational power of the prover.

When the execution of the verifier algorithm stops the following conditions are required to hold:

- (Completeness) If the tuple  $x \in \Sigma^*$  is a word in language  $L$  and both prover and verifier follow the protocol, the verifier outputs `accept`.
- (Soundness) If the tuple  $x \in \Sigma^*$  is not a word in language  $L$  and the verifier follows the protocol, the verifier outputs `reject`, except with some small probability.

In addition, a proof system is called **zero-knowledge** if the verifier learns nothing about  $x$  other than  $x \in L$ .

The previous definition of proof systems is very general, and many subclasses of proving systems are known in the field. The type of languages that a proof system can support crucially depends on the abilities of the verifier (for example, whether it can make random choices) or on the nature and number of the messages that can be exchanged. If the system only requires to send a single message from the prover to the verifier, the proof system is called **non-interactive**, because no interaction other than sending the actual proof is required. In contrast, any other proof system is called **interactive**.

A proof system is usually called **succinct** if the size of the proof is shorter than the witness necessary to generate the proof. Moreover, a proof system is called **computationally sound** if soundness only holds under the assumption that the computational capabilities of the prover are polynomially bound. To distinguish general proofs from computationally sound proofs, the latter are often called **arguments**. Zero-knowledge, succinct, non-interactive arguments of knowledge claims are often abbreviated **zk-SNARKs**.

*Example 138 (Constructive Proofs for Algebraic Circuits).* To formalize our previous notion of constructive proofs for algebraic circuits, let  $\mathbb{F}$  be a finite field, and let  $C(\mathbb{F})$  be an algebraic circuit over  $\mathbb{F}$  with associated language  $L_{C(\mathbb{F})}$ . A non-interactive proof system for  $L_{C(\mathbb{F})}$  is given by the following two algorithms:

Given some instance  $I$ , the prover algorithm  $P$  uses its unlimited computational power to compute a witness  $W$  such that the pair  $(I; W)$  is a valid assignment to  $C(\mathbb{F})$  whenever the circuit is satisfiable for  $I$ . The prover then sends the constructive proof  $(I; W)$  to the verifier.

On receiving a message  $(I; W)$ , the verifier algorithm  $V$  assigns the constructive proof  $(I; W)$  to circuit  $C(\mathbb{F})$ , and decides whether the assignment is valid by executing all gates in the circuit. The runtime is polynomial in the number of gates. If the assignment is valid, the verifier returns `accepts`, if not, it returns `reject`.

To see that this proof system has the completeness and soundness properties, let  $C(\mathbb{F})$  be a circuit of the field  $\mathbb{F}$ , and let  $I$  be an instance. The circuit may or may not have a witness  $W$  such that  $(I; W)$  is a valid assignment to  $C(\mathbb{F})$ .

If no  $W$  exists,  $I$  is not part of any word in  $L_{C(\mathbb{F})}$ , and there is no way for  $P$  to generate a valid assignment. It follows that the verifier will not accept any claimed proof sent by  $P$ , which implies that the system has **soundness**.

If, on the other hand,  $W$  exists and  $P$  is honest,  $P$  can use its unlimited computational power to compute  $W$  and send  $(I; W)$  to  $V$ , which  $V$  will accept in polynomial time. This implies that the system has **completeness**.

The system is non-interactive because the prover only sends a single message to the verifier, which contains the proof itself. Because in this simple system the witness itself is the proof, the proof system is **not** succinct.

## 8.2 The “Groth16” Protocol

In chapter 6, we have introduced algebraic circuits, their associated rank-1 constraint systems and their induced quadratic arithmetic programs. These models define formal languages, and

check  
reference

associated memberships and knowledge claims can be constructively proofed by executing the circuit to compute a solution to its associated R1CS. The solution can then be transformed into a polynomial such that the polynomial is divisible by another polynomial if and only if the solution is correct.

In [\[1\]](#), Jens Groth provides a method that can transform those proofs into zero-knowledge succinct non-interactive arguments of knowledge. Assuming that the pairing groups  $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, b)$  are given, the arguments are of constant size and consist of 2 elements from  $\mathbb{G}_1$  and a single element from  $\mathbb{G}_2$ , regardless of the size of the witness. They are zero-knowledge in the sense that the verifier learns nothing about the witness beside the fact that the instance-witness pair is a proper word in the language of the problem.

Verification is non-interactive and needs to compute a number of exponentiations proportional to the size of the instance, together with 3 group pairings in order to check a single equation.

The generated argument is perfectly zero-knowledge has perfect completeness and soundness in the generic bilinear group model, assuming the existence of a trusted third party that executes a preprocessing phase to generate a **common reference string** and a **simulation trapdoor**. This party must be trusted to delete the simulation trapdoor, since everyone in possession of it can simulate proofs.

To be more precise, let  $R$  be a rank-1 constraint system defined over some finite field  $\mathbb{F}_r$ . Then **Groth\_16 parameters** for  $R$  are given by the following set:

$$\text{Groth\_16} - \text{Param}(R) = (r, \mathbb{G}_1, \mathbb{G}_2, e(\cdot, \cdot), g_1, g_2) \quad (8.1)$$

In the equation above,  $\mathbb{G}_1$  and  $\mathbb{G}_2$  are finite cyclic groups of order  $r$ ,  $g_1$  is a generator of  $\mathbb{G}_1$ ,  $g_2$  is a generator of  $\mathbb{G}_2$  and  $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$  is a non-degenerate, bilinear pairing for some target group  $\mathbb{G}_T$ . In real-world applications, the parameter set is usually agreed on in advance.

Given some Groth\_16 parameters, a **Groth\_16 protocol** is then a quadruple of probabilistic polynomial algorithms (SETUP, PROVE, VFY, SIM) such that the following conditions hold:

- (Setup-Phase):  $(CRS, \tau) \leftarrow \text{Setup}(R)$ : Algorithm Setup takes the R1CS  $R$  as input and computes a common reference string  $CRS$  and a simulation trapdoor  $\tau$ .
- (Prover-Phase):  $\pi \leftarrow \text{Prove}(R, CRS, I, W)$ : Given a constructive proof  $(I, W)$  for  $R$ , algorithm Prove takes the R1CS  $R$ , the common reference string  $CRS$  and the constructive proof  $(I, W)$  as input and computes an zk-SNARK  $\pi$ .
- Verify:  $\{\text{accept}, \text{reject}\} \leftarrow \text{Vfy}(R, CRS, I, \pi)$ : Algorithm Vfy takes the R1CS  $R$ , the common reference string  $CRS$ , the instance  $I$  and the zk-SNARK  $\pi$  as input and returns `reject` or `accept`.
- $\pi \leftarrow \text{Sim}(R, \tau, CRS, I)$ : Algorithm Sim takes the R1CS  $R$ , the common reference string  $CRS$ , the simulation trapdoor  $\tau$  and the instance  $I$  as input and returns a zk-SNARK  $\pi$ .

We will explain these algorithms together with detailed examples in the remainder of this section.

Assuming a trusted third party for the setup, the protocol is able to compute a zk-SNARK from a constructive proof for  $R$ , provided that  $r$  is sufficiently large, and, in particular, larger than the number of constraints in the associated R1CS.

**Example 139** (The 3-Factorization Problem). Consider the 3-factorization problem from 109 and its associated algebraic circuit and rank-1 constraint system from 6.8. In this example,

we want to agree on a parameter set  $(R, r, \mathbb{G}_1, \mathbb{G}_2, e(\cdot, \cdot), g_1, g_2)$  in order to use the Groth\_16 protocol for our 3-factorization problem.

To find proper parameters, first observe that the circuit XXX, as well as its associated R1CS  $R_{3, \text{fac\_zk}}$  ex:3-factorization-r1cs and the derived QAP 6.14, are defined over the field  $\mathbb{F}_{13}$ . We therefore have  $r = 13$  and need pairing groups  $\mathbb{G}_1$  and  $\mathbb{G}_2$  of order 13.

We know from 5.4 that the moon-math curve BLS6\_6 has two subgroups  $\mathbb{G}_1[13]$  and  $\mathbb{G}_2[13]$ , which are both of order 13. The associated Weil pairing  $b$  (5.45) is a proper bilinear map. We therefore choose those groups and the Weil pairing together with the generators  $g_1 = (13, 15)$  and  $g_2 = (7v^2, 16v^3)$  of  $\mathbb{G}_1[13]$  and  $\mathbb{G}_2[13]$ , as a parameter:

$$\text{Groth\_16} - \text{Param}(R_{3, \text{fac\_zk}}) = (r, \mathbb{G}_1[13], \mathbb{G}_2[13], e(\cdot, \cdot), (13, 15), (7v^2, 16v^3))$$

It should be noted that our choice is not unique. Every pair of finite cyclic groups of order 13 that has a proper bilinear pairing qualifies as a Groth\_16 parameter set. The situation is similar to real-world applications, where SNARKs with equivalent behavior are defined over different curves, used in different applications.

**The Setup Phase** To generate zk-SNARKs from constructive knowledge proofs in the Groth16 protocol, a preprocessing phase is required. This has to be executed a single time for every rank-1 constraint system and any associated quadratic arithmetic program. The outcome of this phase is a common reference string that prover and verifier need in order to generate and verify the zk-SNARK. In addition, a simulation trapdoor is produced that can be used to simulate proofs.

To be more precise, let  $L$  be a language defined by some rank-1 constraint system  $R$  such that a constructive proof of knowledge for an instance  $(I_1, \dots, I_n)$  in  $L$  consists of a witness  $(W_1, \dots, W_m)$ . Let  $QAP(R) = \{T \in \mathbb{F}[x], \{A_j, B_j, C_j \in \mathbb{F}[x]\}_{j=0}^{n+m}\}$  be a quadratic arithmetic program associated to  $R$ , and let  $\{\mathbb{G}_1, \mathbb{G}_2, e(\cdot, \cdot), g_1, g_2, \mathbb{F}_r\}$  be the set of Groth\_16 parameters.

The setup phase then samples 5 random, **inverible** elements  $\alpha, \beta, \gamma, \delta$  and  $s$  from the scalar field  $\mathbb{F}_r$  of the protocol and outputs the **simulation trapdoor**  $\tau$ :

$$\tau = (\alpha, \beta, \gamma, \delta, s) \quad (8.2)$$

In addition, the setup phase uses those 5 random elements together with the two generators  $g_1$  and  $g_2$  and the quadratic arithmetic program to generate a **common reference string**  $CRS_{QAP} = (CRS_{\mathbb{G}_1}, CRS_{\mathbb{G}_2})$  of language  $L$ :

$$CRS_{\mathbb{G}_1} = \left\{ \begin{array}{l} g_1^\alpha, g_1^\beta, g_1^\delta, \left( g_1^{s^j}, \dots \right)_{j=0}^{\deg(T)-1}, \left( g_1^{\frac{\beta \cdot A_j(s) + \alpha \cdot B_j(s) + C_j(s)}{\gamma}}, \dots \right)_{j=0}^n \\ \left( g_1^{\frac{\beta \cdot A_{j+n}(s) + \alpha \cdot B_{j+n}(s) + C_{j+n}(s)}{\delta}}, \dots \right)_{j=1}^m, \left( g_1^{\frac{s^j \cdot T(s)}{\delta}}, \dots \right)_{j=0}^{\deg(T)-2} \end{array} \right\}$$

$$CRS_{\mathbb{G}_2} = \left\{ g_2^\beta, g_2^\gamma, g_2^\delta, \left( g_2^{s^j}, \dots \right)_{j=0}^{\deg(T)-1} \right\}$$

Common reference strings depend on the simulation trapdoor, and are therefore not unique to the problem. Any language can have more than one common reference string. The size of a common reference string is linear in the size of the instance and the size of the witness.

If a simulation trapdoor  $\tau = (\alpha, \beta, \gamma, \delta, s)$  is given, we call the element  $s$  a **secret evaluation point** of the protocol, because if  $\mathbb{F}_r$  is the scalar field of the finite cyclic groups  $\mathbb{G}_1$  and  $\mathbb{G}_2$ , then

5808 a key feature of any common reference string is that it provides data to compute the evaluation  
 5809 of any polynomial  $P \in \mathbb{F}_r[x]$  of degree  $\deg(P) < \deg(T)$  at the point  $s$  in the exponent of the  
 5810 generator  $g_1$  or  $g_2$ , without knowing  $s$ .

To be more precise, let  $s$  be the secret evaluation point and let  $P(x) = a_0 \cdot x^0 + a_1 \cdot x^1 + \dots + a_k \cdot x^k$  be a polynomial of degree  $k < \deg(T)$  with coefficients in  $\mathbb{F}_r$ . Then we can compute  $g_1^{P(s)}$  without knowing what the actual value of  $s$  is:

$$\begin{aligned} g_1^{P(s)} &= g_1^{a_0 \cdot s^0 + a_1 \cdot s^1 + \dots + a_k \cdot s^k} \\ &= g_1^{a_0 \cdot s^0} \cdot g_1^{a_1 \cdot s^1} \cdot \dots \cdot g_1^{a_k \cdot s^k} \\ &= \left(g_1^{s^0}\right)^{a_0} \cdot \left(g_1^{s^1}\right)^{a_1} \cdot \dots \cdot \left(g_1^{s^k}\right)^{a_k} \end{aligned}$$

5811 In this expression, all group points  $g_1^{s^j}$  are part of the common reference string, hence, they can  
 5812 be used to compute the result. The same holds true for the evaluation of  $g_2^{P(s)}$ , since the  $\mathbb{G}_2$  part  
 5813 of the common reference string contains the points  $g_2^{s^j}$ .

5814 In real-world applications, the simulation trapdoor is often called the **toxic waste** of the  
 5815 setup-phase, while a common reference string is also-called the pair of **prover and verifier**  
 5816 **key**.

explain  
why

5817 In order to make the protocol secure, the setup needs to be executed in a way that guarantees  
 5818 that the simulation trapdoor is deleted. Anyone in possession of it can generate arguments  
 5819 without knowledge of a constructive proof. The most simple approach to achieving deletion of  
 5820 the toxic waste is by a so-called **trusted third party**, where the trust assumption is that that  
 5821 the party generates the common reference string precisely as defined and deletes the simulation  
 5822 backdoor afterwards.

5823 However, as trusted third parties are not easy to find, more sophisticated protocols exist  
 5824 in real-world applications. They execute the setup phase as a multi party computation, where  
 5825 the proper execution can be publicly verified and the simulation trapdoor is deleted if at least  
 5826 one participant deletes their individual contribution to the randomness. Each participant only  
 5827 possesses a fraction of the simulation trapdoor, so it can only be recovered if all participants  
 5828 collude and share their fraction.

*Example 140* (The 3-factorization Problem). To see how the setup phase of a Groth\_16 zk-SNARK can be computed, consider the 3-factorization problem from 109 and the parameters from page 193. As we have seen in 6.14, an associated quadratic arithmetic program is given as follows:

$$\begin{aligned} QAP(R_{3, fac\_zk}) &= \{x^2 + x + 9, \\ &\quad \{0, 0, 6x + 10, 0, 0, 7x + 4\}, \{0, 0, 0, 6x + 10, 7x + 4, 0\}, \{0, 7x + 4, 0, 0, 0, 6x + 10\}\} \end{aligned}$$

To transform this QAP into a common reference string, we choose the field elements  $\alpha = 6$ ,  $\beta = 5$ ,  $\gamma = 4$ ,  $\delta = 3$ ,  $s = 2$  from  $\mathbb{F}_{13}$ . In real-world applications, it is important to sample those values randomly from the scalar field, but in our approach, we choose those non-random values to make them more memorizable, which helps in pen-and-paper computations. Our simulation trapdoor is then given as follows:

$$\tau = (6, 5, 4, 3, 2)$$

5829 We keep this secret in order to simulate proofs later on, but we are careful though to hide  $\tau$   
 5830 from anyone who hasn't read this book. Then we instantiate the common reference string XXX

4 ex-  
amples  
have the  
same title.  
Change it  
to be dis-  
tinct

check  
reference

add refer-  
ence

check  
reference

add refer-  
ence

5831 from those values. Since our groups are subgroups of the  $\text{BLS}_{6\_6}$  elliptic curve, we use scalar  
 5832 product notation instead of exponentiation.

To compute the  $\mathbb{G}_1$  part of the common reference string, we use the logarithmic order of the group  $\mathbb{G}_1$  XXX, the generator  $g_1 = (13, 15)$ , as well as the values from the simulation backdoor. Since  $\deg(T) = 2$ , we get the following:

add reference

$$\begin{aligned} [\alpha]g_1 &= [6](13, 15) = (27, 34) \\ [\beta]g_1 &= [5](13, 15) = (26, 34) \\ [\delta]g_1 &= [3](13, 15) = (38, 15) \end{aligned}$$

To compute the rest of the  $\mathbb{G}_1$  part of the common reference string, we expand the indexed tuples and insert the secret random elements from the simulation backdoor. We get the following:

$$\begin{aligned} \left( [s^j]g_1, \dots \right)_{j=0}^1 &= \left( [2^0](13, 15), [2^1](13, 15) \right) \\ &= \left( (13, 15), (33, 34) \right) \\ \left( \left[ \frac{\beta A_j(s) + \alpha B_j(s) + C_j(s)}{\gamma} \right]g_1, \dots \right)_{j=0}^1 &= \left( \left[ \frac{5A_0(2) + 6B_0(2) + C_0(2)}{4} \right](13, 15), \right. \\ &\quad \left. \left[ \frac{5A_1(2) + 6B_1(2) + C_1(2)}{4} \right](13, 15) \right) \\ \left( \left[ \frac{\beta A_{j+n}(s) + \alpha B_{j+n}(s) + C_{j+n}(s)}{\delta} \right]g_1, \dots \right)_{j=1}^4 &= \left( \left[ \frac{5A_2(2) + 6B_2(2) + C_2(2)}{3} \right](13, 15), \right. \\ &\quad \left[ \frac{5A_3(2) + 6B_3(2) + C_3(2)}{3} \right](13, 15), \\ &\quad \left[ \frac{5A_4(2) + 6B_4(2) + C_4(2)}{3} \right](13, 15), \\ &\quad \left. \left[ \frac{5A_5(2) + 6B_5(2) + C_6(2)}{3} \right](13, 15) \right) \\ \left( \left[ \frac{s^j \cdot T(s)}{\delta} \right]g_1 \right)_{j=0}^0 &= \left( \left[ \frac{2^0 \cdot T(2)}{3} \right](13, 15) \right) \end{aligned}$$

To compute the curve points on the right side of these expressions, we need the polynomials from the associated quadratic arithmetic program and evaluate them on the secret point  $s = 2$ .



Since  $4^{-1} = 10$  and  $3^{-1} = 9$  in  $\mathbb{F}_{13}$ , we get the following:

$$\left[ \frac{5A_0(2) + 6B_0(2) + C_0(2)}{4} \right](13, 15) = [(5 \cdot 0 + 6 \cdot 0 + 0) \cdot 10](13, 15) = [0](13, 15) =$$

$\emptyset$

$$\left[ \frac{5A_1(2) + 6B_1(2) + C_1(2)}{4} \right](13, 15) = [(5 \cdot 0 + 6 \cdot 0 + (7 \cdot 2 + 4)) \cdot 10](13, 15) = [11](13, 15) =$$

(33, 9)

$$\left[ \frac{5A_2(2) + 6B_2(2) + C_2(2)}{3} \right](13, 15) = [(5 \cdot (6 \cdot 2 + 10) + 6 \cdot 0 + 0) \cdot 9](13, 15) = [2](13, 15) =$$

(33, 34)

$$\left[ \frac{5A_3(2) + 6B_3(2) + C_3(2)}{3} \right](13, 15) = [(5 \cdot 0 + 6 \cdot (6 \cdot 2 + 10) + 0) \cdot 9](13, 15) = [5](13, 15) =$$

(26, 34)

$$\left[ \frac{5A_4(2) + 6B_4(2) + C_4(2)}{3} \right](13, 15) = [(5 \cdot 0 + 6 \cdot (7 \cdot 2 + 4) + 0) \cdot 9](13, 15) = [10](13, 15) =$$

(38, 28)

$$\left[ \frac{5A_5(2) + 6B_5(2) + C_5(2)}{3} \right](13, 15) = [(5 \cdot (7 \cdot 2 + 4) + 6 \cdot 0 + 0) \cdot 9](13, 15) = [4](13, 15) =$$

(35, 28)

$$\left[ \frac{2^0 \cdot T(2)}{3} \right](13, 15) = [1 \cdot (2^2 + 2 + 9) \cdot 9](13, 15) = [5](13, 15) =$$

(26, 34)

Putting all those values together, we see that the  $\mathbb{G}_1$  part of the common reference string is given by the following set of 12 points from the  $\text{BLS}_{6\_6}$  13-torsion group  $\mathbb{G}_1$ :

$$CRS_{\mathbb{G}_1} = \left\{ \begin{array}{l} (27, 34), (26, 34), (38, 15), \left( (13, 15), (33, 34) \right), \left( \emptyset, (33, 9) \right) \\ \left( (33, 34), (26, 34), (38, 28), (35, 28) \right), \left( (26, 34) \right) \end{array} \right\}$$

To compute the  $\mathbb{G}_2$  part of the common reference string, we use the logarithmic order of the group  $\mathbb{G}_2$  XXX, the generator  $g_2 = (7v^2, 16v^3)$ , as well as the values from the simulation backdoor. Since  $\deg(T) = 2$ , we get the following:

$$[\beta]g_2 = [5](7v^2, 16v^3) = (16v^2, 28v^3)$$

$$[\gamma]g_2 = [4](7v^2, 16v^3) = (37v^2, 27v^3)$$

$$[\delta]g_2 = [3](7v^2, 16v^3) = (42v^2, 16v^3)$$

To compute the rest of the  $\mathbb{G}_2$  part of the common reference string, we expand the indexed tuple and insert the secret random elements from the simulation backdoor. We get the following:

$$\begin{aligned} \left( [s^j]g_2, \dots \right)_{j=0}^1 &= ([2^0](7v^2, 16v^3), [2^1](7v^2, 16v^3)) \\ &= ((7v^2, 16v^3), (10v^2, 28v^3)) \end{aligned}$$

Putting all these values together, we see that the  $\mathbb{G}_2$  part of the common reference string is given by the following set of 5 points from the  $\text{BLS}_{6\_6}$  13-torsion group  $\mathbb{G}_2$ :

$$CRS_{\mathbb{G}_2} = \left\{ (16v^2, 28v^3), (37v^2, 27v^3), (42v^2, 16v^3), (7v^2, 16v^3), (10v^2, 28v^3) \right\}$$

add reference



Given the simulation trapdoor  $\tau$  and the quadratic arithmetic program 6.14, the associated common reference string of the 3-factorization problem is as follows:

check  
reference

$$\begin{aligned} CRS_{\mathbb{G}_1} &= \left\{ (27, 34), (26, 34), (38, 15), \left( (13, 15), (33, 34) \right), \left( \mathcal{O}, (33, 9) \right) \right\} \\ &\quad \left\{ \left( (33, 34), (26, 34), (38, 28), (35, 28) \right), \left( (26, 34) \right) \right\} \\ CRS_{\mathbb{G}_2} &= \left\{ (16v^2, 28v^3), (37v^2, 27v^3), (42v^2, 16v^3), \left( 7v^2, 16v^3 \right), (10v^2, 28v^3) \right\} \end{aligned}$$

We then publish this data to everyone who wants to participate in the generation of a zk-SNARK or its verification in the 3-factorization problem.

To understand how this common reference string can be used to evaluate polynomials at the secret evaluation point in the exponent of a generator, let's assume that we have deleted the simulation trapdoor. In that case, we have no way to know the secret evaluation point anymore, hence, we cannot evaluate polynomials at that point. However, we can evaluate polynomials of smaller degree than the degree of the target polynomial in the exponent of both generators at that point.

To see that, consider e.g. the polynomials  $A_2(x) = 6x + 10$  and  $A_5(x) = 7x + 4$  from the QAP of this problem. To evaluate these polynomials in the exponent of  $g_1$  and  $g_2$  at the secret point  $s$  without knowing the value of  $s$  (which is 2), we can use the common reference string and equation XXX. Using the scalar product notation instead of exponentiation, we get the following:

add refer-  
ence

$$\begin{aligned} [A_2(s)]g_1 &= [6 \cdot s^1 + 10 \cdot s^0]g_1 \\ &= [6](33, 34) + [10](13, 15) & \# [s^0]g_1 = (13, 15), [s^1]g_1 = (33, 34) \\ &= [6 \cdot 2](13, 15) + [10](13, 15) = [9](13, 15) & \# \text{logarithmic order on } \mathbb{G}_1 \\ &= (35, 15) \\ [A_5(s)]g_1 &= [7 \cdot s^1 + 4 \cdot s^0]g_1 \\ &= [7](33, 34) + [4](13, 15) \\ &= [7 \cdot 2](13, 15) + [4](13, 15) = [5](13, 15) \\ &= (26, 34) \end{aligned}$$

Indeed, we are able to evaluate the polynomials in the exponent at a secret evaluation point, because that point is encrypted in the curve point  $(33, 34)$  and its secrecy is protected by the discrete logarithm assumption. Of course, in our computation, we recovered the secret point  $s = 2$ , but that was only possible because we have a group of logarithmic order in order to simplify our pen-and-paper computations. Such an order is infeasible for computing in cryptographically secure curves. We can do the same computation on  $\mathbb{G}_2$  and get the following:

$$\begin{aligned} [A_2(s)]g_2 &= [6 \cdot s^1 + 10 \cdot s^0]g_2 \\ &= [6](10v^2, 28v^3) + [10](7v^2, 16v^3) \\ &= [6 \cdot 2](7v^2, 16v^3) + [10](7v^2, 16v^3) = [9](7v^2, 16v^3) \\ &= (37v^2, 16v^3) \\ [A_5(s)]g_2 &= [7 \cdot s^1 + 4 \cdot s^0]g_2 \\ &= [7](10v^2, 28v^3) + [4](7v^2, 16v^3) \\ &= [7 \cdot 2](7v^2, 16v^3) + [4](7v^2, 16v^3) = [5](7v^2, 16v^3) \\ &= (16v^2, 28v^3) \end{aligned}$$

Apart from the target polynomial  $T$ , all other polynomials of the quadratic arithmetic program can be evaluated in the exponent this way.

**The Prover Phase** Given some rank-1 constraint system  $R$  and instance  $I = (I_1, \dots, I_n)$ , the task of the prover phase is to convince any verifier that a prover knows a witness  $W$  to instance  $I$  such that  $(I; W)$  is a word in the language  $L_R$  of the system, without revealing anything about  $W$ .

To achieve this in the Groth\_16 protocol, we assume that any prover has access to the rank-1 constraint system of the problem, in addition to some algorithm that tells the prover how to compute constructive proofs for the R1CS. In addition, the prover has access to a common reference string and its associated quadratic arithmetic program.

In order to generate a zk-SNARK for this instance, the prover first computes a valid constructive proof as explained in XXX, that is, the prover generates a proper witness  $W = (W_1, \dots, W_m)$  such that  $(I_1, \dots, I_n; W_1, \dots, W_m)$  is a solution to the rank-1 constraint system  $R$ .

The prover then uses the quadratic arithmetic program and computes the polynomial  $P_{(I;W)}$ , as explained in 6.15. They then divide  $P_{(I;W)}$  by the target polynomial  $T$  of the quadratic arithmetic program. Since  $P_{(I;W)}$  is constructed from a valid solution to the R1CS, we know from 6.15 that it is divisible by  $T$ . This implies that polynomial division of  $P$  by  $T$  generates another polynomial  $H := P/T$ , with  $\deg(H) < \deg(T)$ .

The prover then evaluates the polynomial  $(H \cdot T)\delta^{-1}$  in the exponent of the generator  $g_1$  at the secret point  $s$ , as explained in XXX. To see how this can be achieved, let  $H(x)$  be the quotient polynomial  $P/T$ :

$$H(x) = H_0 \cdot x^0 + H_1 \cdot x^1 + \dots + H_k \cdot x^k \quad (8.3)$$

To evaluate  $H \cdot T$  at  $s$  in the exponent of  $g_1$ , the prover uses the common reference string and computes as follows:

$$g_1^{\frac{H(s) \cdot T(s)}{\delta}} = \left(g_1^{\frac{s^0 \cdot T(s)}{\delta}}\right)^{H_0} \cdot \left(g_1^{\frac{s^1 \cdot T(s)}{\delta}}\right)^{H_1} \dots \left(g_1^{\frac{s^k \cdot T(s)}{\delta}}\right)^{H_k}$$

After this has been done, the prover samples two random field elements  $r, t \in \mathbb{F}_r$ , and uses the common reference string, the instance variables  $I_1, \dots, I_n$  and the witness variables  $W_1, \dots, W_m$  to compute the following curve points:

$$\begin{aligned} g_1^W &= \left(g_1^{\frac{\beta \cdot A_{1+n}(s) + \alpha \cdot B_{1+n}(s) + C_{1+n}(s)}{\delta}}\right)^{W_1} \dots \left(g_1^{\frac{\beta \cdot A_{m+n}(s) + \alpha \cdot B_{m+n}(s) + C_{m+n}(s)}{\delta}}\right)^{W_m} \\ g_1^A &= g_1^\alpha \cdot g_1^{A_0(s)} \cdot \left(g_1^{A_1(s)}\right)^{I_1} \dots \left(g_1^{A_n(s)}\right)^{I_n} \cdot \left(g_1^{A_{n+1}(s)}\right)^{W_1} \dots \left(g_1^{A_{n+m}(s)}\right)^{W_m} \cdot \left(g_1^\delta\right)^r \\ g_1^B &= g_1^\beta \cdot g_1^{B_0(s)} \cdot \left(g_1^{B_1(s)}\right)^{I_1} \dots \left(g_1^{B_n(s)}\right)^{I_n} \cdot \left(g_1^{B_{n+1}(s)}\right)^{W_1} \dots \left(g_1^{B_{n+m}(s)}\right)^{W_m} \cdot \left(g_1^\delta\right)^t \\ g_2^B &= g_2^\beta \cdot g_2^{B_0(s)} \cdot \left(g_2^{B_1(s)}\right)^{I_1} \dots \left(g_2^{B_n(s)}\right)^{I_n} \cdot \left(g_2^{B_{n+1}(s)}\right)^{W_1} \dots \left(g_2^{B_{n+m}(s)}\right)^{W_m} \cdot \left(g_2^\delta\right)^t \\ g_1^C &= g_1^W \cdot g_1^{\frac{H(s) \cdot T(s)}{\delta}} \cdot \left(g_1^A\right)^r \cdot \left(g_1^B\right)^t \cdot \left(g_1^\delta\right)^{-r \cdot t} \end{aligned}$$

In this computation, the group elements  $g_1^{A_j(s)}$ ,  $g_1^{B_j(s)}$  and  $g_2^{B_j(s)}$  can be derived from the common reference string and the quadratic arithmetic program of the problem, as we have seen in XXX. In fact, those points only have to be computed once, and can be published and reused

for multiple proof generations because they are the same for all instances and witnesses. All other group elements are part of the common reference string.

After all these computations have been done, a valid zero-knowledge succinct non-interactive argument of knowledge  $\pi$  in the Groth\_16 protocol is given by the following three curve points:

$$\pi = (g_1^A, g_1^C, g_2^B) \quad (8.4)$$

As we can see, a Groth\_16 zk-SNARK consists of 3 curve points, two points from  $\mathbb{G}_1$  and 1 point from  $\mathbb{G}_2$ . The argument is specifically designed this way because, in typical applications,  $\mathbb{G}_1$  is a torsion group of an elliptic curve over some prime field, while  $\mathbb{G}_2$  is a subgroup of a torsion group over an extension field. Elements from  $\mathbb{G}_1$  therefore need less space to be stored, and computations in  $\mathbb{G}_1$  are typically faster than in  $\mathbb{G}_2$ .

Since the witness is encoded in the exponent of a generator of a cryptographically secure elliptic curve, it is hidden from anyone but the prover. Moreover, since any proof is randomized by the occurrence of the random field elements  $r$  and  $t$ , proofs are not unique to any given witness. This is an important feature because, if all proofs for the same witness would be the same, knowledge of a witness would destroy the zero-knowledge property of those proofs.

*Example 141* (The 3-factorization Problem). To see how a prover might compute a zk-SNARK, consider the 3-factorization problem from 109, our protocol parameters from XXX as well as the common reference string from XXX.

Our task is to compute a zk-SNARK for the instance  $I_1 = 11$  and its constructive proof  $(W_1, W_2, W_3, W_4) = (2, 3, 4, 6)$  as computed in XXX. As we know from 6.15, the associated polynomial  $P_{(I;W)}$  of the quadratic arithmetic program from XXX is given by the following equation:

$$P_{(I;W)} = x^2 + x + 9$$

Since  $P_{(I;W)}$  is identical to the target polynomial  $T(x) = x^2 + x + 9$  in this example, we know from XXX that the quotient polynomial  $H = P/T$  is the constant degree 0 polynomial:

$$H(x) = H_0 \cdot x^0 = 1 \cdot x^0$$

We therefore use  $[\frac{s^0 \cdot T(s)}{\delta}]_{g_1} = (26, 34)$  from our common reference string XXX of the 3-factorization problem and compute as follows:

$$\begin{aligned} [\frac{H(s) \cdot T(s)}{\delta}]_{g_1} &= [H_0](26, 34) = [1](26, 34) \\ &= (26, 34) \end{aligned}$$

In the next step, we have to compute all group elements required for a proper Groth16 zk-SNARK. We start with  $g_1^W$ . Using scalar products instead of the exponential notation, and  $\oplus$  for the group law on the BLS6\_6 curve, we have to compute the point  $[W]g_1$ :

$$\begin{aligned} [W]g_1 &= [W_1]g_1 \frac{\beta \cdot A_2(s) + \alpha \cdot B_2(s) + C_2(s)}{\delta} \oplus [W_2]g_1 \frac{\beta \cdot A_3(s) + \alpha \cdot B_3(s) + C_3(s)}{\delta} \oplus [W_3]g_1 \frac{\beta \cdot A_4(s) + \alpha \cdot B_4(s) + C_4(s)}{\delta} \\ &\quad \oplus [W_4]g_1 \frac{\beta \cdot A_5(s) + \alpha \cdot B_5(s) + C_5(s)}{\delta} \end{aligned}$$

To compute this point, we have to remember that a prover should not be in possession of the simulation trapdoor, hence, they do not know what  $\alpha$ ,  $\beta$ ,  $\delta$  and  $s$  are. In order to compute this group element, the prover therefore needs the common reference string. Using the logarithmic order from XXX and the witness, we get the following:

check  
reference

add refer-  
ence

add refer-  
ence

add refer-  
ence

check  
reference

add refer-  
ence

add refer-  
ence

add refer-  
ence

add refer-  
ence

$$\begin{aligned}
[W]g_1 &= [2](33, 34) \oplus [3](26, 34) \oplus [4](38, 28) \oplus [6](35, 28) \\
&= [2 \cdot 2](13, 15) \oplus [3 \cdot 5](13, 15) \oplus [4 \cdot 10](13, 15) \oplus [6 \cdot 4](13, 15) \\
&= [2 \cdot 2 + 3 \cdot 5 + 4 \cdot 10 + 6 \cdot 4](13, 15) = [5](13, 15) \\
&= (26, 34)
\end{aligned}$$

5886 In a next step, we compute  $g_1^A$ . We sample the random point  $r = 11$  from  $\mathbb{F}_{13}$ , using scalar  
5887 products instead of the exponential notation, and  $\oplus$  for the group law on the BLS6\_6 curve.  
5888 We then have to compute the following expression:

$$\begin{aligned}
[A]g_1 &= [\alpha]g_1 \oplus [A_0(s)]g_1 \oplus [I_1][A_1(s)]g_1 \oplus [W_1][A_2(s)]g_1 \oplus [W_2][A_3(s)]g_1 \\
&\quad \oplus [W_3][A_4(s)]g_1 \oplus [W_4][A_5(s)]g_1 \oplus [r][\delta]g_1
\end{aligned}$$

Since we don't know what  $\alpha$ ,  $\delta$  and  $s$  are, we look up  $[\alpha]g_1$  and  $[\delta]g_1$  from the common reference string. Recall from XXX that we can evaluate  $[A_j(s)]g_1$  without knowing the secret evaluation point  $s$ . According to XXX, we have  $[A_2(s)]g_1 = (35, 15)$ ,  $[A_5(s)]g_1 = (26, 34)$  and  $[A_j(s)]g_1 = \mathcal{O}$  for all other indices  $0 \leq j \leq 5$ . Since  $\mathcal{O}$  is the neutral element on  $\mathbb{G}_1$ , we get the following:

$$\begin{aligned}
[A]g_1 &= (27, 34) \oplus \mathcal{O} \oplus [11]\mathcal{O} \oplus [2](35, 15) \oplus [3]\mathcal{O} \oplus [4]\mathcal{O} \oplus [6](26, 34) \oplus [11](38, 15) \\
&= (27, 34) \oplus [2](35, 15) \oplus [6](26, 34) \oplus [11](38, 15) \\
&= [6](13, 15) \oplus [2 \cdot 9](13, 15) \oplus [6 \cdot 5](13, 15) \oplus [11 \cdot 3](13, 15) \\
&= [6 + 2 \cdot 9 + 6 \cdot 5 + 11 \cdot 3](13, 15) = [9](13, 15) \\
&= (35, 15)
\end{aligned}$$

5889 In order to compute the two curve points  $[B]g_1$  and  $[B]g_2$ , we sample another random element  
5890  $t = 4$  from  $\mathbb{F}_{13}$ . Using the scalar product instead of the exponential notation, and  $\oplus$  for the group  
5891 law on the BLS6\_6 curve, we have to compute the following expressions:

$$\begin{aligned}
[B]g_1 &= [\beta]g_1 \oplus [B_0(s)]g_1 \oplus [I_1][B_1(s)]g_1 \oplus [W_1][B_2(s)]g_1 \oplus [W_2][B_3(s)]g_1 \\
&\quad \oplus [W_3][B_4(s)]g_1 \oplus [W_4][B_5(s)]g_1 \oplus [t][\delta]g_1 \\
[B]g_2 &= [\beta]g_2 \oplus [B_0(s)]g_2 \oplus [I_1][B_1(s)]g_2 \oplus [W_1][B_2(s)]g_2 \oplus [W_2][B_3(s)]g_2 \\
&\quad \oplus [W_3][B_4(s)]g_2 \oplus [W_4][B_5(s)]g_2 \oplus [t][\delta]g_2
\end{aligned}$$

Since we don't know what  $\beta$ ,  $\delta$  and  $s$  are, we look up the associated group elements from the common reference string. Recall from XXX that we can evaluate  $[B_j(s)]g_1$  without knowing the secret evaluation point  $s$ . Since  $B_3 = A_2$  and  $B_4 = A_5$ , we have  $[B_3(s)]g_1 = (35, 15)$ ,  $[B_4(s)]g_1 = (26, 34)$  according to XXX, and  $[B_j(s)]g_1 = \mathcal{O}$  for all other indices  $0 < j < 5$ . Since  $\mathcal{O}$  is the neutral element on  $\mathbb{G}_1$ , we get the following:

$$\begin{aligned}
[B]g_1 &= (26, 34) \oplus \mathcal{O} \oplus [11]\mathcal{O} \oplus [2]\mathcal{O} \oplus [3](35, 15) \oplus [4](26, 34) \oplus [6]\mathcal{O} \oplus [4](38, 15) \\
&= (26, 34) \oplus [3](35, 15) \oplus [4](26, 34) \oplus [4](38, 15) \\
&= [5](13, 15) \oplus [3 \cdot 9](13, 15) \oplus [4 \cdot 5](13, 15) \oplus [4 \cdot 3](13, 15) \\
&= [5 + 3 \cdot 9 + 4 \cdot 5 + 4 \cdot 3](13, 15) = [12](13, 15) \\
&= (13, 28)
\end{aligned}$$

$$\begin{aligned}
 [B]g_2 &= (16v^2, 28v^3) \oplus \mathcal{O} \oplus [11]\mathcal{O} \oplus [2]\mathcal{O} \oplus [3](37v^2, 16v^3) \oplus [4](16v^2, 28v^3) \oplus [6]\mathcal{O} \oplus [4](42v^2, 16v^3) \\
 &= (16v^2, 28v^3) \oplus [3](37v^2, 16v^3) \oplus [4](16v^2, 28v^3) \oplus [4](42v^2, 16v^3) \\
 &= [5](7v^2, 16v^3) \oplus [3 \cdot 9](7v^2, 16v^3) \oplus [4 \cdot 5](7v^2, 16v^3) \oplus [4 \cdot 3](7v^2, 16v^3) \\
 &= [5 + 3 \cdot 9 + 4 \cdot 5 + 4 \cdot 3](7v^2, 16v^3) = [12](7v^2 + 16v^3) \\
 &= (7v^2, 27v^3)
 \end{aligned}$$

In a last step, we combine the previous computations to compute the point  $[C]g_1$  in the group  $\mathbb{G}_1$  as follows:

$$\begin{aligned}
 [C]g_1 &= [W]g_1 \oplus \left[ \frac{H(s) \cdot T(s)}{\delta} \right]g_1 \oplus [t][A]g_1 \oplus [r][B]g_1 \oplus [-r \cdot t][\delta]g_1 \\
 &= (26, 34) \oplus (26, 34) \oplus [4](35, 15) \oplus [11](13, 28) \oplus [-11 \cdot 4](38, 15) \\
 &= [5](13, 15) \oplus [5](13, 15) \oplus [4 \cdot 9](13, 15) \oplus [11 \cdot 12](13, 15) \oplus [-11 \cdot 4 \cdot 3](13, 15) \\
 &= [5 + 5 + 4 \cdot 9 + 11 \cdot 12 - 11 \cdot 4 \cdot 3](13, 15) = [7](13, 15) \\
 &= (27, 9)
 \end{aligned}$$

Given the instance  $I_1 = 11$ , we can now combine these computations and see that the following 3 curve points are a zk-SNARK for the witness  $(W_1, W_2, W_3, W_4) = (2, 3, 4, 6)$ :

$$\pi = ((35, 15), (27, 9), (7v^2, 27v^3))$$

5892 We can now publish this zk-SNARK, or send it to a designated verifier. Note that, if we had  
 5893 sampled different values for  $r$  and  $t$ , we would have computed a different SNARK for the same  
 5894 witness. The SNARK, therefore, hides the witness perfectly, which means that it is impossible  
 5895 to reconstruct the witness from the SNARK.

5896 **The Verification Phase** Given some rank-1 constraint system  $R$ , instance  $I = (I_1, \dots, I_n)$  and  
 5897 zk-SNARK  $\pi$ , the task of the verification phase is to check that  $\pi$  is indeed an argument for  
 5898 a constructive proof. Assuming that the simulation trapdoor does not exist anymore and the  
 5899 verification checks the proof, the verifier can be convinced that someone knows a witness  $W =$   
 5900  $(W_1, \dots, W_m)$  such that  $(I; W)$  is a word in the language of  $R$ .

To achieve this in the Groth16 protocol, we assume that any verifier is able to compute the pairing map  $e(\cdot, \cdot)$  efficiently, and has access to the common reference string used to produce the SNARK  $\pi$ . In order to verify the SNARK with respect to the instance  $(I_1, \dots, I_n)$ , the verifier computes the following curve point:

$$g_1^I = \left( g_1^{\frac{\beta \cdot A_0(s) + \alpha \cdot B_0(s) + C_0(s)}{\gamma}} \right) \cdot \left( g_1^{\frac{\beta \cdot A_1(s) + \alpha \cdot B_1(s) + C_1(s)}{\gamma}} \right)^{I_1} \cdots \left( g_1^{\frac{\beta \cdot A_n(s) + \alpha \cdot B_n(s) + C_n(s)}{\gamma}} \right)^{I_n}$$

5901 With this group element, the verifier is able to verify the SNARK  $\pi = (g_1^A, g_1^C, g_2^B)$  by checking  
 5902 the following equation using the pairing map:

$$e(g_1^A, g_2^B) = e(g_1^\alpha, g_2^\beta) \cdot e(g_1^I, g_2^\gamma) \cdot e(g_1^C, g_2^\delta) \quad (8.5)$$

5903 If the equation holds true, the SNARK is accepted. If the equation does not hold, the  
 5904 SNARK is rejected.

*Remark 7.* We know from chapter 5 that computing pairings in cryptographically secure pairing groups is computationally expensive. As we can see, in the Groth16 protocol, 3 pairings are required to verify the SNARK, because the pairing  $e(g_1^\alpha, g_2^\beta)$  is independent of the proof, meaning that can be computed once and then stored as an amendment to the verifier key.

check  
reference

In ?, the author showed that 2 is the minimal amount of pairings that any protocol with similar properties has to use. This protocol is therefore close to the theoretical minimum. In the same paper, the author outlined an adaptation that only uses 2 pairings. However, that reduction comes with the price of much more overhead computation. Having 3 pairings is therefore a compromise that gives the overall best performance. To date, the Groth16 protocol is the most efficient in its class.

*Example 142* (The 3-factorization Problem). To see how a verifier might check a zk-SNARK for some given instance  $I$ , consider the 3-factorization problem from 109, our protocol parameters from XXX, the common reference string from XXX as well as the zk-SNARK  $\pi = ((35, 15), (27, 9), (7v^2, 27v^3))$ , which claims to be an argument of knowledge for a witness for the instance  $I_1 = 11$ .

check  
reference

In order to verify the zk-SNARK for that instance, we first compute the curve point  $g_1^I$ . Using scalar products instead of the exponential notation, and  $\oplus$  for the group law on the BLS6\_6 curve, we have to compute the point  $[I]g_1$  as follows:

add refer-  
ence

add refer-  
ence

$$[I]g_1 = \left[ \frac{\beta \cdot A_0(s) + \alpha \cdot B_0(s) + C_0(s)}{\gamma} \right]_{g_1} \oplus [I_1] \left[ \frac{\beta \cdot A_1(s) + \alpha \cdot B_1(s) + C_1(s)}{\gamma} \right]_{g_1}$$

To compute this point, we have to remember that a verifier should not be in possession of the simulation trapdoor, which means that they do not know what  $\alpha$ ,  $\beta$ ,  $\gamma$  and  $s$  are. In order to compute this group element, the verifier therefore needs the common reference string. Using the logarithmic order from XXX and instance  $I_1$ , we get the following:

add refer-  
ence

$$\begin{aligned} [I]g_1 &= \left[ \frac{\beta \cdot A_0(s) + \alpha \cdot B_0(s) + C_0(s)}{\gamma} \right]_{g_1} \oplus [I_1] \left[ \frac{\beta \cdot A_1(s) + \alpha \cdot B_1(s) + C_1(s)}{\gamma} \right]_{g_1} \\ &= \mathcal{O} \oplus [11](33, 9) \\ &= [11 \cdot 11](13, 15) = [4](13, 15) \\ &= (35, 28) \end{aligned}$$

In the next step, we have to compute all the pairings involved in equation XXX. Using the logarithmic order on  $\mathbb{G}_1$  and  $\mathbb{G}_2$  as well as the bilinearity property of the pairing map we get the following:

add refer-  
ence

$$\begin{aligned}
e([A]_{g_1}, [B]_{g_2}) &= e((35, 15), (7v^2, 27v^3)) = e([9](13, 15), [12](7v^2, 16v^3)) \\
&= e((13, 15), (7v^2, 16v^3))^{9 \cdot 12} \\
&= e((13, 15), (7v^2, 16v^3))^{108} \\
e([\alpha]_{g_1}, [\beta]_{g_2}) &= e((27, 34), (16v^2, 28v^3)) = e([6](13, 15), [5](7v^2, 16v^3)) \\
&= e((13, 15), (7v^2, 16v^3))^{6 \cdot 5} \\
&= e((13, 15), (7v^2, 16v^3))^{30} \\
e([I]_{g_1}, [\gamma]_{g_2}) &= e((35, 28), (37v^2, 27v^3)) = e([4](13, 15), [4](7v^2, 16v^3)) \\
&= e((13, 15), (7v^2, 16v^3))^{4 \cdot 4} \\
&= e((13, 15), (7v^2, 16v^3))^{16} \\
e([C]_{g_1}, [\delta]_{g_2}) &= e((27, 9), (42v^2, 16v^3)) = e([7](13, 15), [3](7v^2, 16v^3)) \\
&= e((13, 15), (7v^2, 16v^3))^{7 \cdot 3} \\
&= e((13, 15), (7v^2, 16v^3))^{21}
\end{aligned}$$

5930 In order to check equation XXX, observe that the target group  $\mathbb{G}_T$  of the Weil pairing is  
 5931 a finite cyclic group of order 13. Exponentiation is therefore done in modular 13 arithmetics.  
 5932 Accordingly, since  $108 \bmod 13 = 4$ , we evaluate the left side of equation XXX as follows:

$$e([A]_{g_1}, [B]_{g_2}) = e((13, 15), (7v^2, 16v^3))^{108} = e((13, 15), (7v^2, 16v^3))^4$$

5933 Similarly, we evaluate the right side of equation XXX using modular 13 arithmetics and the  
 5934 exponential law  $a^x \cdot a^y = a^{x+y}$ :

$$\begin{aligned}
&e([\alpha]_{g_1}, [\beta]_{g_2}) \cdot e([I]_{g_1}, [\gamma]_{g_2}) \cdot e([C]_{g_1}, [\delta]_{g_2}) = \\
&e((13, 15), (7v^2, 16v^3))^{30} \cdot e((13, 15), (7v^2, 16v^3))^{16} \cdot e((13, 15), (7v^2, 16v^3))^{21} = \\
&e((13, 15), (7v^2, 16v^3))^4 \cdot e((13, 15), (7v^2, 16v^3))^3 \cdot e((13, 15), (7v^2, 16v^3))^8 = \\
&e((13, 15), (7v^2, 16v^3))^{4+3+8} = \\
&e((13, 15), (7v^2, 16v^3))^2
\end{aligned}$$

5935 As we can see, both the left and the right side of equation XXX are identical, which implies  
 5936 that the verification process accepts the simulated proof.

5937 **NOTE: UNFORTUNATELY NOT! :-( (HENCE THERE IS AN ERROR SOMEWHERE ...**  
 5938 **NEED TO FIX IT AFTER VACATION**

5939 **Proof Simulation** During the execution of a setup phase, a common reference string is gen-  
 5940 erated, along with a simulation trapdoor, the latter of which must be deleted at the end of the  
 5941 setup-phase. As an alternative, a more complicated multi-party protocol like [XXX] can be  
 5942 used to split the knowledge of the simulation trapdoor among many different parties.

5943 In this paragraph, we will show why knowledge of the simulation trapdoor is problematic,  
 5944 and how it can be used to generate zk-SNARKs for a given instance without any knowledge or  
 5945 the existence of associated witness.

5946 To be more precise, let  $I$  be an instance for some R1CS language  $L_R$ . We call a zk-SNARK  
 5947 for  $L_R$  **forged** or **simulated** if it passes a verification but its generation does not require the  
 5948 existence of a witness  $W$  such that  $(I; W)$  is a word in  $L_R$ .



To see how simulated zk-SNARKs can be computed, assume that a forger has knowledge of proper Groth\_16 parameters, a quadratic arithmetic program of the problem, a common reference string and its associated simulation trapdoor  $\tau$ :

$$\tau = (\alpha, \beta, \gamma, \delta, s) \quad (8.6)$$

Given some instance  $I$ , the forger’s task is to generate a zk-SNARK for this instance that passes the verification process, without having access to any other zk-SNARKs for this instance and without knowledge of a valid witness  $W$ .

To achieve this in the Groth\_16 protocol, the forger can use the simulation trapdoor in combination with the QAP and two arbitrary field elements  $A$  and  $B$  from the scalar field  $\mathbb{F}_r$  of the pairing groups to  $g_1^C$  compute for the instance  $(I_1, \dots, I_n)$  as follows:

$$g_1^C = g_1^{\frac{A \cdot B}{\delta}} \cdot g_1^{-\frac{\alpha \cdot \beta}{\delta}} \cdot g_1^{-\frac{\beta A_0(s) + \alpha B_0(s) + C_0(s)}{\delta}} \cdot \left( g_1^{-\frac{\beta A_1(s) + \alpha B_1(s) + C_1(s)}{\delta}} \right)^{I_1} \cdots \left( g_1^{-\frac{\beta A_n(s) + \alpha B_n(s) + C_n(s)}{\delta}} \right)^{I_n}$$

The forger then publishes the zk-SNARK  $\pi_{\text{forged}} = (g_1^A, g_1^C, g_2^B)$ , which will pass the verification process and is computable without the existence of a witness  $(W_1, \dots, W_m)$ .

To see that the simulation trapdoor is necessary and sufficient to compute the simulated proof  $\pi_{\text{forged}}$ , first observe that both generators  $g_1$  and  $g_2$  are known to the forger, as they are part of the common reference string, encoded as  $g_1^{s^0}$  and  $g_2^{s^0}$ . The forger is therefore able to compute  $g_1^{A \cdot B}$ . Moreover, since the forger knows  $\alpha, \beta, \delta$  and  $s$  from the trapdoor, they are able to compute all factors in the computation of  $g_1^C$ .

If, on the other hand, the simulation trapdoor is unknown, it is not possible to compute  $g_1^C$ , since, for example, the computational Diffie-Hellman assumption makes the derivation of  $g_1^{\alpha \cdot \beta}$  from  $g_1^\alpha$  and  $g_1^\beta$  infeasible.

**Example 143** (The 3-factorization Problem). To see how a forger might simulate a zk-SNARK for some given instance  $I$ , consider the 3-factorization problem from 109, our protocol parameters from XXX, the common reference string from XXX and the simulation trapdoor  $\tau = (6, 5, 4, 3, 2)$  of that CRS.

In order to forge a zk-SNARK for instance  $I_1 = 11$ , we don’t need a constructive proof for the associated rank-1 constraint system, which implies that we don’t have to execute the circuit  $C_{3.\text{fac}}(\mathbb{F}_{13})$ . Instead, we have to choose 2 arbitrary elements  $A$  and  $B$  from  $\mathbb{F}_{13}$ , and compute  $g_1^A, g_2^B$  and  $g_1^C$  as defined in XXX. We choose  $A = 9$  and  $B = 3$ , and, since  $\delta^{-1} = 3$ , we compute as follows:

$$\begin{aligned} [A]g_1 &= [9](13, 15) = (35, 15) \\ [B]g_2 &= [3](7v^2, 16v^3) = (42v^2, 16v^3) \\ [C]g_1 &= \left[ \frac{A \cdot B}{\delta} \right]g_1 \oplus \left[ -\frac{\alpha \cdot \beta}{\delta} \right]g_1 \oplus \left[ -\frac{\beta A_0(s) + \alpha B_0(s) + C_0(s)}{\delta} \right]g_1 \oplus \\ &\quad [I_1] \left[ -\frac{\beta A_1(s) + \alpha B_1(s) + C_1(s)}{\delta} \right]g_1 \\ &= [(9 \cdot 3) \cdot 9](13, 15) \oplus [-(6 \cdot 5) \cdot 9](13, 15) \oplus [0](13, 15) \oplus [11][-(7 \cdot 2 + 4) \cdot 9](13, 15) \\ &= [9](13, 15) \oplus [3](13, 15) \oplus [12](13, 15) = [11](13, 15) \\ &= (33, 9) \end{aligned}$$

check  
reference

add refer-  
ence

add refer-  
ence

add refer-  
ence



This is all we need to generate our forged proof for the 3-factorization problem. We publish the simulated zk-SNARK:

$$\pi_{fake} = ((35, 15), (33, 9), (42v^2, 16v^3))$$

Despite the fact that this zk-SNARK was generated without knowledge of a proper witness, it is indistinguishable from a zk-SNARK that proves knowledge of a proper witness.

To see that, we show that our forged SNARK passes the verification process. In order to verify  $\pi_{fake}$ , we proceed as in XXX, and compute the curve point  $g_1^I$  for the instance  $I_1 = 11$ . Since the instance is the same as in example XXX, we can parallel the computation from XXX:

$$\begin{aligned} [I]g_1 &= \left[ \frac{\beta \cdot A_0(s) + \alpha \cdot B_0(s) + C_0(s)}{\gamma} \right]g_1 \oplus [I_1] \left[ \frac{\beta \cdot A_1(s) + \alpha \cdot B_1(s) + C_1(s)}{\gamma} \right]g_1 \\ &= (35, 28) \end{aligned}$$

In a next step we have to compute all the pairings involved in equation XXX. Using the logarithmic order on  $\mathbb{G}_1$  and  $\mathbb{G}_2$  as well as the bilinearity property of the pairing map we get

$$\begin{aligned} e([A]g_1, [B]g_2) &= e((35, 15), (42v^2, 16v^3)) = e([9](13, 15), [3](7v^2, 16v^3)) \\ &= e((13, 15), (7v^2, 16v^3))^{9 \cdot 3} \\ &= e((13, 15), (7v^2, 16v^3))^{27} \\ e([\alpha]g_1, [\beta]g_2) &= e((27, 34), (16v^2, 28v^3)) = e([6](13, 15), [5](7v^2, 16v^3)) \\ &= e((13, 15), (7v^2, 16v^3))^{6 \cdot 5} \\ &= e((13, 15), (7v^2, 16v^3))^{30} \\ e([I]g_1, [\gamma]g_2) &= e((35, 28), (37v^2, 27v^3)) = e([4](13, 15), [4](7v^2, 16v^3)) \\ &= e((13, 15), (7v^2, 16v^3))^{4 \cdot 4} \\ &= e((13, 15), (7v^2, 16v^3))^{16} \\ e([C]g_1, [\delta]g_2) &= e((33, 9), (42v^2, 16v^3)) = e([11](13, 15), [3](7v^2, 16v^3)) \\ &= e((13, 15), (7v^2, 16v^3))^{11 \cdot 3} \\ &= e((13, 15), (7v^2, 16v^3))^{33} \end{aligned}$$

In order to check equation XXX, observe that the target group  $\mathbb{G}_T$  of the Weil pairing is a finite cyclic group of order 13. Exponentiation is therefore done in modular 13 arithmetics. Using this, we evaluate the left side of equation XXX as follows:

$$e([A]g_1, [B]g_2) = e((13, 15), (7v^2, 16v^3))^{27} = e((13, 15), (7v^2, 16v^3))^1$$

since  $27 \bmod 13 = 1$ . Similarly, we evaluate the right side of equation XXX using modular 13 arithmetics and the exponential law  $a^x \cdot a^y = a^{x+y}$ . We get

$$\begin{aligned} e([\alpha]g_1, [\beta]g_2) \cdot e([I]g_1, [\gamma]g_2) \cdot e([C]g_1, [\delta]g_2) &= \\ e((13, 15), (7v^2, 16v^3))^{30} \cdot e((13, 15), (7v^2, 16v^3))^{16} \cdot e((13, 15), (7v^2, 16v^3))^{33} &= \\ e((13, 15), (7v^2, 16v^3))^4 \cdot e((13, 15), (7v^2, 16v^3))^3 \cdot e((13, 15), (7v^2, 16v^3))^7 &= \\ e((13, 15), (7v^2, 16v^3))^{4+3+7} &= \\ e((13, 15), (7v^2, 16v^3))^1 & \end{aligned}$$

5982 As we can see, both the left and the right side of equation XXX are identical, which implies  
5983 that the verification process accepts the simulated proof.  $\pi_{fake}$  therefore convinces the veri-  
5984 fier that a witness to the 3-factorization problem exists. However, no such witness was really  
5985 necessary to generate the proof.

add refer-  
ence

## 5986 **Chapter 9**

## 5987 **Exercises and Solutions**

5988 TODO: All exercises we provided should have a solution, which we give here in all detail.