Contents

1 Division, and Prime Numbers

1.1 Division

Theorem 1.1. *For every $a \in \mathbb{Z}$ and $b \geq 1$, there exists some q and r such that*

$$a = qb + r$$

Proof. Consider $X = \{a - bx : x \in \mathbb{Z}\}_n\mathbb{N}$, where "$_n\mathbb{N}$" indicates that we are restricting the set to its nonnegative elements. We want to claim: a) the set is nonempty, and b) the set has a lower bound.

For $a \geq 0$, then $x = 0$ yields $a \in X$, and if a is negative, then $x = a$ yields $(a - ba) = a(1 - b)$. a is negative and $b \geq 1$, so $a(1 - b)$ will be a negative number multiplied by something less than or equal to 0, thus $a(1 - b)$ is nonnegative.

So X is always nonempty. Let r be the smallest element of X, and let q be such that

$$a = qb + r$$

Which implies $a - qb = r$. Now, we show that r is, at most, $(b - 1)$ (i.e., $r \leq (b - 1)$.

Suppose, to obtain a contradiction, that $r \geq b$. Let $s = r - b$. Then, $s \geq 0$, because $r \geq b$, and $s = a - (q + 1)b \in X$. So, we have now found a new smallest element of X than r, which is a contradiction. ■

Associated with this operation is a relation.

1.2 Divisibility Relation

Definition 1.1. $b|a$ (read "b divides a" or "b is a divisor of a" or "a is a multiple of b") is defined by

$$b|a \iff a = bx \text{ for some } x \in \mathbb{Z}$$

This is equivalent (if b is positive) to saying the remainder is zero independent of the signs of a and b. From this definition, we can say $0|0$. If $0|a$, then a *must* be zero—there is no integer x such that $0x = a \neq 0$. A few things to note:

1. The divides relation is reflexive: $a|a \forall a \in \mathbb{Z}$, with $q = 1$.
2. The divides relation is transitive: if $a|b$ and $b|c$, then $a|c$ $\forall a, b, c \in \mathbb{Z}$. Basically, we multiply by something, and then something else.
3. If $d|a$, then $d|(a \cdot x) \forall x \in \mathbb{Z}$.
4. If $d|a$ and $d|b$, then $d|(a + b)$
5. It follows 3. and 4. that if $d|a$ and $d|b$, then $d|(ax + by) \forall x, y \in \mathbb{Z}$. This can be read as "$d$ divides any integer linear combination of a and b."

1.3 Primes

The number 1 can be thought of as the "basic building block of positive integers by addition." I.e., if we have any positive integer x, we can construct x by adding sufficiently many values of 1 together. In a similar sense, primes are "the building blocks of positive integers by multiplication!"

Definition 1.2. Prime: a number $a \geq 2$ is said to be **prime** if the only positive integers that divide a are 1 and a. Note that we say here that we specify $a \geq 2$, so 1 is not a prime. In a moment, we'll see that this is to make the Fundamental Theorem of Arithmetic cleaner.

Definition 1.3. Composite: a number $a \geq 2$ is **composite** if $a = bc$ for some $b \geq 2,\ c \geq 2$. Basically, composite means that a number can be expressed as the product of two numbers, which can themselves be either prime or composite.

On the next page is a list of the primes between 0 and 900, with the primes in black. Grey numbers are composite, and 0 and 1, being special cases, are written in blue. If you can find a formula/pattern that will generate the n^{th} prime, you will likely win the Fields medal and go down in history as having made the single largest contribution to mathematics that ever was. But for now, we go on to prove a Lemma, to use in the proof of the fundamental theorem of arithmetic.

Lemma 1.2. *For every integer $a \geq 2$, we have $p|a$ for some prime p.*

Proof. (By contradiction): Suppose, to obtain a contradiction, that Lemma 1.2 is false, and let $a \geq 2$ be the smallest integer not divisible by any prime.

The number a cannot itself be prime, because if it were, it would divide itself (because the division relation is reflexive), and would thus be divisible by a prime.

Then a must be composite. Let $a = bc$ with $b \geq 2$ and $c \geq 2$. Then b is smaller than a, so $p|b$ for some prime p (this is because we defined a as the SMALLEST integer for which the Lemma fails, so any integer smaller than a must satisfy the Lemma). But then, since $b|a$, we have $p|a$, a contradiction. So, there does not exist a smallest counterexample to the Lemma, so it must hold for all $a \geq 2$. ■

Now, we use Lemma 1.2 to prove a theorem.

Theorem 1.3. *There are (countably) infinitely many primes. I.e., if P is the set of primes, $|P| = \aleph_0$.*

Proof. (By contradiction): We will only prove the infinite part, not the countably infinite part. Suppose, to obtain a contradiction, that there are only finitely many primes, and list them

$$(p_1, p_2, \ldots, p_k)$$

Consider the number $N = p_1 p_2 \cdots p_k + 1$. N is at least 2, because the smallest prime is $p_1 = 2$, so by the lemma, we have $q|N$ for some prime q. The prime q cannot be among the primes $p_1 p_2 \cdots p_k$, because since N leaves a remainder of 0 when divided by q, but leaves a remainder of 1 when divided by any $p_i \in \{p_1, p_2, \ldots, p_k\}$. Thus, q is a prime not among the $p_1 \ldots p_k$, a contradiction. ■

1.4 Remarks

- Divisibility is Reflexive and Transitive.
- However, it's not quite antisymmetric; for instance $-1|1$ and $1|-1$, but $-1 \neq 1$.
- Something that's reflexive and transitive is called a **pre-order**. If we add in antisymmetric, we get an **order**.
- If $(a|b \wedge b|a)$, we define this as $a \equiv b$. Note, this is an equivalence relation (i.e., it is reflexive, transitive, and symmetric).
- Equivalence classes partition a "universe of discourse" into sets of elements related by an equivalence relation. Associates are members of the same equivalence classes.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107
108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125
126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161
162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179
180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197
198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215
216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233
234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251
252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269
270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287
288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305
306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323
324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341
342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359
360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377
378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395
396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413
414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431
432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449
450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467
468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485
486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503
504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521
522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539
540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557
558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575
576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593
594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611
612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629
630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647
648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665
666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683
684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701
702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719
720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737
738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755
756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773
774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791
792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809
810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827
828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845
846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863
864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881
882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899

2 The Fundamental Theorem of Arithmetic, GCD, and LCM

2.1 The Fundamental Theorem of Arithmetic and Corollaries

Theorem 2.1 (The Fundamental Theorem of Arithmetic)**.** *Every integer $a \geq 1$ is the product of the primes in a unique multiset of primes.*

Existence proof. (By Strong Induction) We first prove the existence part—that is, that a has a prime factorization

$$a = p_1 p_2 \dots p_i \text{ for primes } p_1, p_2, \dots, p_i$$

We proceed by strong Induction. For the base case, $a = 1$, we can take $i = 0$, i.e. the number corresponding to the empty multiset $\langle\rangle$. The product of the empty multiset is 1, so 1 can be expressed as a multiset of primes, namely the empty multiset. For the inductive step, we now consider $a \geq 2$ (as we have disposed of 1). We assume the existence of a prime factorization for all positive integers strictly less than a, and prove for a. If $a \geq 2$ is prime, then we can take $i = 1$, and $p_1 = a$. I.e., we can express a as the product of a multiset just containing itself. Otherwise, if a is composite, then we can express a as the product of two numbers bc with $b \geq 2,\ c \geq 2$. Because neither b nor c is 1, then we must have that $a > b$ and $a > c$, because b and c at the very least divide a in two. Thus, by the inductive hypothesis, b and c have prime factorizations

$$b = q_1 q_2 \dots q_j \qquad\qquad c = r_1 r_2 \dots r_k$$

And thus

$$a = q_1 q_2 \dots q_j r_1 r_2 \dots r_k = b \cdot c$$

Thus, by the Principle of Mathematical Induction (strong version), every integer $a \geq 1$ can be written as the product of the primes in a multiset of primes. ■

Uniqueness proof. (By Contradiction) Now, we prove uniqueness. Suppose, to obtain a contradiction, that uniqueness fails, and by the well ordering principle, we can focus on a number n, the smallest possitive integer that has two distinct factorizations.

$$n = p_1 p_2 \dots p_i \qquad\qquad n = q_1 q_2 \dots q_j$$

None of the p's can be the same as any of the q's, otherwise we could divide both factorizations of n by the common prime, and obtain a smaller counterexample.

Without loss of generality, p_1 is the smallest of p's $p_1 \dots p_i$, and q_1 is the smallest of the q's $q_1 \dots q_j$, and $p_1 < q_1$. (N.B.—this is a perfectly fine thing to stipulate, and **does not affect the validity of the proof or restrict our values of n in any way.** It is equivalent to stating "call the smallest of the p's p_1 and the second smallest p_2 ... and do the same with the q's, then switch which ones are labled as p or q depending on which has the smaller smallest element.)

Now, consider $m = p_1(q_2 \dots q_j)$. Then, we have $1 \leq m < n$, because p_1 is strictly less than q_1. Thus, $n - m$, which is

$$n - m = (q_1 - p_1) q_2 \dots q_j$$

Is strictly smaller than n, so it must have a unique factorization into primes. We will obtain a contradiction by finding two different factorizations for $n - m$.

Since $p_1 | m$ and $p_1 | n$, it divides their integer linear combination (i.e., $p | (n - m)$), so we have

$$(n - m) = p_1(r_1 \dots r_k) \tag{1}$$

When $r_1 \dots r_k$ is a factorization of $\frac{n-m}{p_1}$. On the other hand, we have

$$(n-m) = s_1 \dots s_\ell q_1 \dots q_j \tag{2}$$

where $s_1 \dots s_\ell$ is a factorization of $q_1 - p_1$. We now now want to find a prime that occurs in (1) but not (2). p_1 can't be any of the q's, as noted before. But also, it's not among the s's, because $p_1 \nmid (q_1 - p_1)$ because $p_1 \nmid q_1$ (no prime divides another prime).

Thus, (1) and (2) are different factorizations of $n - m$, so we've found a new smallest number that cannot be written as a unique product of primes, a contradiction. Thus, every number $a \geq 1$ can be written as the product of the primes in a *unique* multiset of primes. ■

Corollary 2.1.1. *Suppose a and b are positive integers, and p is prime. If $p|ab$, then either $p|a$, or $p|b$, or both. It's essential that p is a prime—for instance, $4|(2 \cdot 6)$, but $4 \nmid 2$, $4 \nmid 6$.*

Proof. Let $a = q_1 \dots q_i$ and $b = r_1 \dots r_j$ be the factorization of a and b into primes. Then,

$$ab = q_1 \dots q_i r_1 \dots r_j \tag{3}$$

is the "unique" factorization of ab. Since $p|ab$, then

$$ab = p(s_1 \dots s_k) \tag{4}$$

where $s_1 \dots s_k$ is the factorization of $\frac{ab}{p}$. Then, p appears in (3) or (4), and thus p divides a or b. (N.B.—that's an inclusive or!) ■

2.2 GCD and LCM

Let's consider the orders of addition and division over the positiver integers.

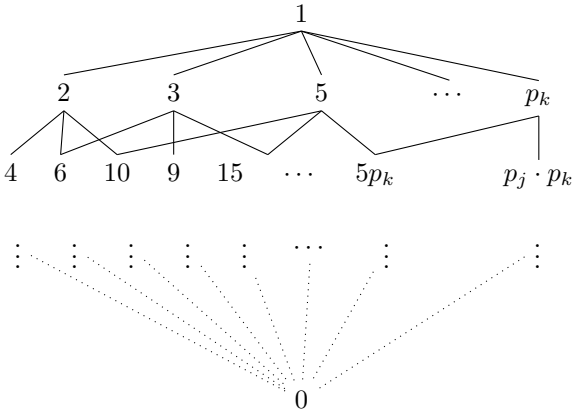

Figure 1: The order of division. Note that numbers in the n^{th} row have n prime factors. Any positive integer divides 0, so 0 is at the "top" (yes it's mirrored here I know) of the order.

Figure 2: The order of addition

Notice that when considering the construction of integers by multiplication, we have to think a lot less linearly. Thus, in the following cases, we'll have to be sure we treat 0 as a special case, so we'll deal initially with values of a that are greater than or equal to 1.

Suppose $a \geq 1$. Then

$$a = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot 5^{\alpha_5} \cdots p^{\alpha_p} \cdots \tag{5}$$

Where the α's are natural numbers greater than or equal to 0, where each α tells us how many times each prime appears in the prime factorization. Note that for $a \in \mathbb{N}$, for any prime p, $\alpha_p \geq 0$, but $\alpha_p \geq 1$ for only finitely many p. Let us define b similarly:

$$b = 2^{\beta_2} \cdot 3^{\beta_3} \cdot 5^{\beta_5} \cdots p^{\beta_p} \cdots \tag{6}$$

Then,

$$ab = 2^{\alpha_2+\beta_2} \cdot 3^{\alpha_3+\beta_3} \cdot 5^{\alpha_5+\beta_5} \cdots p^{\alpha_p+\beta_p} \cdots \tag{7}$$

Furthermore, $b|a$ iff $\beta_p \leq \alpha_p \ \ \forall p$ where p is a prime, and in this case, if $b|a$, then $\frac{a}{b}$ is an integer, and we can find it in a similar manner to (7) by taking

$$\frac{a}{b} = 2^{\alpha_2-\beta_2} \cdot 3^{\alpha_3-\beta_3} \cdot 5^{\alpha_5-\beta_5} \cdots p^{\alpha_p-\beta_p} \cdots \tag{8}$$

Given a and b, we can introduce the **least common multiple** of a and b (denoted $[a, b]$), the smallest positive integer for which a and b are both divisors

Definition 2.1 (Least Common Multiple)**.**

$$[a, b] = 2^{\max(\alpha_2,\beta_2)} \cdot 3^{\max(\alpha_3,\beta_3)} \cdot 5^{\max(\alpha_5,\beta_5)} \cdots p^{\max(\alpha_p,\beta_p)} \cdots \tag{9}$$

So $a|[a, b]$ and $b|[a, b]$. Note that if $a|c$ and $b|c$, then it must be true that $[a, b]|c$.

Similarly, we introduce the **greatest common divisor** of a and b (denoted (a, b)), the largest positive integer that divides both a and b

Definition 2.2 (Greatest Common Divisor)**.**

$$(a, b) = 2^{\min(\alpha_2,\beta_2)} \cdot 3^{\min(\alpha_3,\beta_3)} \cdot 5^{\min(\alpha_5,\beta_5)} \cdots p^{\min(\alpha_p,\beta_p)} \cdots \tag{10}$$

$(a, b)|a$ and $(a, b)|b$, so if we have some $c|a$ and $c|b$, then surely $c|(a, b)$. Now, we turn our attention to the special case of 0. How does 0 fit into gcd and lcm? We can't plug 0 into (5); the lowest we can go there is 1, because all the α must be nonnegative. Well, the least common multiple of a number a and 0 is just going to be 0–a divides 0, and 0 divides 0. So, we have

$$[a, 0] = [0, a] = 0$$

Which we can generalize further, but won't. With gcd of a number a and 0, well, any number divides 0, so then

$$(a, 0) = (0, a) = a$$

Finally, note that $\min(\alpha + \beta) + \max(\alpha + \beta) = \alpha + \beta$, so therefore

$$[a, b](a, b) = ab$$

Finally, if $(a, b) = 1$, then the prime factor multisets are disjoint; we have to go all the way down to 1 on the multiplicative order diagram to find a common factor! We have a special term for this:

Definition 2.3 (Relatively Prime)**.** $a \perp b$ (read "a is relatively prime to b") if $(a, b) = 1$ i.e. a and b share no prime factors.

2.3 Remarks

Not much to say here this time. But, some fun facts about primes—as k gets large, the k^{th} prime (denoted p_k) approaches $k \log k$! Furthermore, $\pi(x)$, the number of primes less than x similarly approaches $\pi(x) \sim \frac{x}{logx}$

3 The Euclidean Algorithm and Modular Arithmetic

3.1 Euclid's Algorithm

There is no efficient algorithm for factorization of numbers into primes. In fact, it's a good thing there aren't—essentially all encryption for sending things like credit card information over the internet to an organization like amazon relies on "scrambling" your traffic information by essentially multiplying by some very very large prime numbers that only you and amazon know. However, there are some efficient algorithms for things like (a, b). One simple (but inefficient) way to find *gcd* would be to just go through all the numbers between 1 and $\frac{1}{2}\max(a, b)$. But, that would be pretty inefficient. As one can probably infer by the name of this section, Euclid found an efficient algorithm for finding (a, b), written below in pseudocode:

```
"""
Without loss of generality, assume a >= b >= 0.  gcd takes two such a and b, and
returns the gcd(a,b).
"""
def gcd(a,b):
  if b == 0:
    return a
  else: # the real work done here!
    find q and r such that a = qb + r with 0<=r<=b-1
    # note that b,r satisifies the argument conditions,
    # and r decreases monotonically!
    return gdc(b,r)
```

Basically, we're taking advantage of the fact that $(a, b) = (b, a - qb)$

3.1.1 Efficiency

For $k \geq 2$, $a = F_{k+2}$ and $b = F_{k+1}$ are the smallest positive integers for which Euclid's Algorithm performs k divisions. We have

$$F_k \sim \frac{1}{\sqrt{5}}(\phi)^k$$

Where ϕ is the golden ratio. $k \sim \log_\phi(2)\log_2(a+1) + O(1)$ That is, the number of calls required will be proportional to the number of bits in the binary representation of the number, rather than to the number itself.

3.2 Diophantine equations

3.2.1 What is a Diophantine Equation anyways?

Definition 3.1 (Diophantine Equations)**.** A *Diophantine equation* is an algebraic equation in which the coefficients are integers, and the unknowns are required to be integers as well.

The simplest Diophantine equation is

$$ax = d$$

Basically, given coefficients $a, b \in \mathbb{Z}$, we want to find integer values of x, which is possible iff $a|b$. That is, $a|b$ is a necessary and sufficient condition to find integer x. However, this equation is pretty restrictive—we can imagine that if we were picking values of a and b somewhat haphazardly, we wouldn't be very likely to get an equation with a valid solution. E.g., we could choose $a = 2, b = 3$, for which there is no $x \in \mathbb{Z}$ that satisfies the equation. In fact, it's pretty obvious that if there *does* exist a solution x, it is the *only* solution. "What a boring equation," you might be thinking to yourself. And you'd be right! Let's move onto something with more solutions.

3.2.2 Bézout's Identity

To make it easier for us to find solutions, we can toss in another variable with another coefficient. For instance, if we toss in a by term, we get what is known as **Bézout's Equation**:

$$ax + by = d \tag{11}$$

Again, given $a, b, d \in \mathbb{Z}$, we want to find $x, y \in \mathbb{Z}$. It'd be nice if we had a little guidance with which to attack this problem—sure, for values like $a = 2, b = 2, d = 4$ the problem might seem trivial, but with larger values like $a = 30127,\ b = 2592,\ d = 79243184$, the problem becomes substantially more difficult. After all, how can we even be sure that a solution exists? The key, as one might expect, lies in the greatest common divisor of a and b, as detailed in the following Theorem:

Theorem 3.1 (Bézout's Theorem)**.** *There exist integers x and y such that $ax+by = d$ if and only if $(a, b)|d$. If such x and y exist, then there are infinitely many solutions.*

Proof. ($\Rightarrow$) If (11) holds (i.e. there is a solution to (11)), then because (a, b) divides a and (a, b) also divides b, then it must divide their integer linear combination, d.

($\Rightarrow$) For the converse, it will suffice to find a solution to $ax + by = (a, b)$. For then, if $d = (a, b)m$, then $axm + bym = d$. To do so, we will modify Euclid's algorithm so that it returns suitable values of x and y, as well as $g = (a, b)$, in a triple (g, x, y).

```
"""
Without loss of generality, assume a >= b >= 0.  gcd takes two such a and b, and
returns the gcd(a,b).
"""
def gcd*(a,b):
  if b == 0:         # if b=0, then we just have the first Diophantine equation, so
    return (a,1,0)   # gcd(a,0) = a, so g is a, then x is 1 and y is 0
  else:
    find q and r such that a = qb + r with 0<=r<=b-1
    (g,x,y) = gcd*(b,r)  # we take the output g,x,and y from calling gcd* on b and r
    return (g,b,x-qy)    # and subtract off the difference, or something.  I think this
                         # will get us to any returned number mod g is 0??
```

Basically, when there is a solution, there are infinitely many: if a or b is 0, then x or y can be given any value (if $a = 0$, we'd vary x as much as we want; if $y = 0$, then we'd mess with b). If neither a nor b is 0, we can add any multiple of b to x, and subtract a corresponding multiple of a from y to keep d at its current value. I.e., we can ensure that

$$\begin{aligned} ax + by &= d \\ a(x + k) + b(y - l) &= d \end{aligned}$$

if we choose k and l such that $ak - bl = 0$, i.e. $ak = bl$ or $\frac{a}{b} = \frac{l}{k}$. If we had $a = 3, b = 12$, and $d = 42$, then one solution would be $3(2) + 12(3) = 42$, but we could also "convert" one of the 12's into 4 3's, by making the coefficient on a $2 + (4)$, then "remove" one of the 12's by making the coefficient $3 - 1 = 2$. Basically, if b and a are thought of as "basis vectors" (although not necessarily linearly independent), we can get to the same point in the span of a and b by writing the same overall linear combination in infinitely many ways. ■

I thought the gcd* argument was hard to follow, so here is a different proof from wikipedia:

Proof. Let S be the set of all positive integer combinations of a and b. S is nonempty, because we can just take $a+b$, flipping the signs on a and b as needed to obtain a positive result. S contains only positive integers, so S is bounded below by 0 and therefore has a smallest element. Let d be the smallest such solution (i.e., d is the smallest integer of the form $ax + by$). Specifically, let

$$d = as + bt \qquad\qquad n = ax + by, \text{ with } n > d$$

Suppose, to obtain a contradiction, that $d \nmid n$. Then, by Euclidean division,

$$\begin{aligned} n &= qd + r, \text{ with } 0 < r < d \\ r &= n - qd \\ &= ax + by - q(as + bt) \\ &= a(x - qs) + b(y - qt) \end{aligned}$$

which is of the form $ax + by$. But $r < d$, a contradiction—thus, $d|n$. ■

3.3 Modular Arithmetic

Let $m \geq 1$ be a positive integer called the *modulus*. We'll write $a \bmod m$ to represent the remainder when a is divided by m. If $a \bmod m = b \bmod m$, then we write

$$a \equiv_m b$$

Read as "a is congruent mod m to b", or "a is congruent to b mod m." Note that this is equivalent to saying $m|(a - b)$, i.e. a and b correspond to an "offset" cycle of m ticks. Let's examine some properties of this relation.

- First of all, $\equiv_m$ is reflexive, because $a \equiv_m a$.
- It is also transitive, because if $(a \equiv_m b) \wedge (b \equiv_m c)$, then $a \equiv_m c$.
- Additionally, it is symmetric, because $a \equiv_m b$ implies that $b \equiv_m a$.
- Therefore, because $\equiv_m$ is reflexive, transitive, and symmetric, it is an **equivalence relation**, and so partitions the "universe of discourse" into **equivalence classes**, i.e. m classes of the form

$$[a]_m = \{b \in \mathbb{Z} : a \equiv_m b\}$$

Let's consider these equivalence classes in more depth. Interestingly, we can do arithmetic on them. For instance,

$$[a]_m + [b]_m = [a + b]_m$$

In fact, this does not depend on the specific values of a and b. Essentially, the contents of the first equivalence class are numbers of the form $a + km$, where a is the remainder of the elements when divided by m (the r in Euclidean division), and km is the qb term. Likewise, all the members of the second equivalence class are of the form $b + lm$. If we take their sum, then we have a number of the form $a + b + km + lm$. When we examine this number mod m, we just get something of the form $a + b \bmod m$! So indeed, the equation holds. Furthermore, we have

$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

To show this, suppose we just examine two representative elements of the same forms as before. We have,

$$\begin{aligned} [a]_m \cdot [b]_m &= [(a + km)(b + lm)]_m \\ &= [ab + alm + bkm + klm^2]_m \\ &= [ab + 0 + 0 + 0]_m \end{aligned}$$

Because any multiple of m is 0 mod m.

3.4 Remarks

- The set of m equivalence classes modulo m, with addition and multiplication as defined above, is denoted $\mathbb{Z}/(m)$, $\mathbb{Z}/m\mathbb{Z}$, or $\mathbb{Z}_m$ (the last of which is read as the "m-adic integers").
- if $d|m$, then surely $a \equiv_m b$ implies $a \equiv_d b$, because we'd still preserve the "offset" of a and b relative to our modulus, we'd just be "resetting" twice as often.

4 Modular Congruence and Modular Equivalence Classes

4.1 Multiplicative Inverses of Equivalence Classes

4.1.1 Recap from last time

- $\equiv_m$ is an equivalence relation, and we can do arithmetic like $+, -$, and $\times$ over equivalence classes. For $-$, we'd just do $[a]_m - [b]_m = [a]_m + [b]_m \cdot [-1]_m$. But can we divide?
- Well, if we can, we probably can't divide by the equivalence class containing 0, at least not if division is defined similarly to the subtraction and multiplication here.

4.1.2 Multiplicative Inverses modulo m

Theorem 4.1 (Multiplicative Inverse of $[a]_m$)**.** *The equivalence class containing a modulo m ($[a]_m$) has a multiplicative inverse if and only if*

$$a \perp m$$

Or, equivalently stated, $(a, m) = 1$ (the gcd of a and m is 1).

($\Rightarrow$)*:* Suppose that $a \perp m$. Then, by Bézout's Theorem, $\exists x$ and y such that

$$ax + my = (a, b) = 1$$

Then $ax \equiv_m 1$, so $[x]$ is a multiplicative inverse of the equivalence class containing a. ■

($\Leftarrow$)*:* Suppose, to obtain a contradiction, that $ax \equiv_m 1$, and $(a, b) = d \geq 2$. Let $q = \frac{m}{d}$. $q \in \mathbb{Z}$ because d must divide m if d is the gcd of a and m. Then

$$1 \leq q \leq m$$

So $q \not\equiv_m 0$. But,

$$\begin{aligned} aq &= a\left(\frac{m}{d}\right) \\ &= \left(\frac{a}{d}\right) m \end{aligned}$$

Which is an integer multiple of m, so $\frac{q}{d}m \equiv_m 0$, and

$$q \equiv_m (ax)q = (aq)x \equiv_m 0$$

A contradiction ■

Multiplicative inverses allow us to solve congruences such as

$$ax \equiv_m b$$

Which, by the theorem, is solvable iff $a \perp m$, in which case the solutions are the elements of $[a]_m^{-1}[b]$.

4.2 The Chinese Remainder Theorem

Theorem 4.2 (The Case of Two Moduli)**.** *Suppose m and n are relatively prime moduli. Then, integers z satisfying the congruences*

$$z \equiv_m a \text{ and } z \equiv_n b \tag{12}$$

all belong to the same equivalence class modulo mn.

i.e., if we find a k that satisfies both congruences, then $k + mn$ satisfies the congruences as well, and so on with $k + cmn$ for any $c \in \mathbb{Z}$. This makes some degree of intuitive sense, because if $z = a \bmod m$, then because mn is a multiple of m, then $z + mn = a \bmod m$ should hold, and the same is true for n. Moreover, if m and n are relatively prime, then their least common multiple is mn. Recalling the fact that the least common multiple of two numbers is the smallest integer for which both m and n are factors, then it makes sense that the residues will only "sync up" every mn numbers. So, uniqueness mod mn seems reasonable. But can we prove it?

Existence. We'll first find α and β such that

$$\begin{aligned} \alpha &\equiv_m 1 \text{ and } \beta \equiv_m 0 \\ \alpha &\equiv_m 0 \text{ and } \beta \equiv_m 1 \end{aligned} \tag{13}$$

Since $m \perp n$, then by Bezout's Theorem, there exist x and y such that

$$mx + ny = 1$$

Let $\alpha = ny$ and $\beta = mx$. Note that α is a multiple of n, so then $\alpha \equiv_n 0$, and β is a multiple of m, so $\beta \equiv_m 0$. Additionally, $mx + ny \bmod n = 1 \bmod n = mx + 0 \equiv_n 1$, and similarly, $mx + ny \equiv_m 1 \equiv_m 0 + ny$, thus $ny \equiv_m 1$ and $mx \equiv_n 1$. Then α and β satisfy (13). Finally, let $z = a\alpha + b\beta$. Then, z satisfies (12). ■

Uniqueness. We have $|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$, because $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \times |\mathbb{Z}_n|$. That is, the set of positive integer residues mod mn is the same size as the set of all possible pairwise combinations of elements where the first is chosen from $\mathbb{Z}_m$ and the second from $\mathbb{Z}_n$[1]. Consider $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, defined by $f([z]_{mn}) \to ([z]_m, [z]_n)$. That is, for every equivalence class mod mn containing some representative element z, we return a tuple containing the equivalence class containg z mod m, and the equivalence class containing z mod n. By the existence proof, we've shown that we can always find some z that satisfies (12). Therefore, f must be onto. Because the domain and codomain are the same size, then f must also be one-to-one. Thus, f is a bijection, and so z is unique modulo mn. ■

4.3 Wilson's Theorem

Theorem 4.3 (Wilson's Theorem)**.** *Suppose p is prime. Then $(p-1)! \equiv_p -1$.*

To prove Wilson's Theorem, we first prove a small lemma.

Lemma 4.4. *Suppose p is prime. Then if $x^2 \equiv_p 1$, then $x \equiv_p \pm 1$.*

Proof of Lemma. We have $x^2 \equiv_p 1$. Subtracting 1 from both sides yields

$$x^2 - 1 \equiv_p 0$$

Because $x^2 - 1$ leaves a residue of 0 mod p, then we must have that $p|(x^2 - 1) = (x - 1)(x + 1)$. By some theorem I forgot, this implies that either $p|(x - 1)$ or $p|(x + 1)$, so therefore $x - 1 \equiv_p 0 \vee x + 1 \equiv_p 0$, and $x \equiv_p 1 \vee x \equiv_p -1$. ■

Now, we can move to the main proof.

Proof. We want to show that the product

$$1 \times 2 \times 3 \times \cdots \times (p-1) \equiv_p -1$$

Note that, by the properties of multiplication mod p, we can rewrite this expression as

$$(1 \bmod p) \times (2 \bmod p) \times \cdots \times ((p-1) \bmod p)$$

[1] Recall that the cartesian product of two sets A and B is defined by $A \times B = \{(a, b) : a \in A, b \in B\}$

Consider the set of all positive residues mod p. All the elements of the set are either their own multiplicative inverses, or they can be paired with another multiplicative inverse also in the set. It must be true that 1 and $(p-1)$ are the only elements that are their own multiplicative inverses, for if x were its own multiplicative inverse, then $x^2 \equiv_p 1$ so $x \equiv_p \pm 1$ (recall that $(p-1) \equiv_p (-1)$). Then, if we evaluate the product, we'll have every element and its inverse pair to yield 1 mod p, except for 1 and $(p-1)$, so we have

$$1 \times 2 \times 3 \times \cdots \times (p-1) \equiv_p 1 \times 1 \times 1 \times \cdots \times 1 \times (p-1)$$
$$\prod_{k=1}^{p-1} k \equiv_p (p-1)$$
$$\prod_{k=1}^{p-1} k \equiv_p -1$$

■

Scholium 1. Suppose n is composite. Then,

$$(n-1)! \not\equiv_n (-1)$$

For $n \neq 1, 0$.

Proof. Since n is composite, let $d|n$ with $2 \leq d \leq n$. Then, $d|(n-1)!$ implying $d \nmid (n-1)! + 1$, which in turn implies that $n \nmid (n-1)! + 1$, so then $(n-1) \not\equiv_n -1$. ■

5 Fermat's Theorem and Primality

5.1 Fermat's Theorem

Theorem 5.1 (Fermat's Theorem)**.** *Let p be prime, and let $a \perp p$. Then*

$$a^{p-1} \equiv_p 1$$

Proof. The numbers

$$\Big(1, 2, \ldots, (p-2), (p-1)\Big)$$

are a permutation of the numbers

$$\Big((a \cdot 1) \bmod p, (a \cdot 2) \bmod p, \ldots, (a(p-1)) \bmod p\Big)$$

Consider the function f where $f : \{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, (p-1)\}$ defined by

$$f(x) = a \cdot x \bmod p$$

Basically, f takes us from the first row to the second row. I claim that f is one-to-one. That is, if $f(x) = f(y)$, then $x = y$. We can multiply both sides by the multiplicative inverse of a because $a \perp p$, so

$$a^{-1}ax \equiv_p a^{-1}ay$$
$$x \equiv_p y$$

We showed in the homework that if the cardinality of the domain of a function equals that of its codomain, then if f is one-to-one, it must also be onto and is therefore a bijection. Note that a bijection between a

set and itself is just a permutation. Then, because the multiplicative order is commutative and associative, then we have

$$\prod_{x=1}^{p-1} x \equiv_p \prod_{x=1}^{p-1} f(x)$$
$$\prod_{x=1}^{p-1} x \equiv_p \prod_{x=1}^{p-1} ax$$
$$\prod_{x=1}^{p-1} x \equiv_p a^{p-1} \left(\prod_{x=1}^{p-1} x \right)$$
$$\cancel{\prod_{x=1}^{p-1} x} \equiv_p a^{p-1} \cancel{\left(\prod_{x=1}^{p-1} x \right)}$$
$$1 \equiv_p a^{p-1}$$

Basically, since there were $p-1$ a's, we just removed them all from the product of x's, and then canceled the product of x's from each side. Note that a must be relatively prime in order for us to show the one-to-one nature of the function, so that is why we require $a \perp p$ in the theorem. ■

Wilson's theorem is inefficient to check. Fermat's theorem, on the other hand, is much more efficient to check. However, Wilson's theorem is a biconditional–i.e., if $(k-1)! \equiv_k -1$, then k *must* be prime. Meanwhile, the converse to Fermat's theorem fails, in a "very spectacular way."

5.2 Modular Exponentiation

Now that we have Fermat's Theorem (which involves powers of a number under some modulus), we seek to define a more computationally feasible way of taking a^n modulo m (for $m \geq 1$)than just raising a to n and then dividing. We can fairly readily define a recursive algorithm to do just that. Suppose $0 \leq a \leq m-1$. This must be true—if it weren't, we could just take the remainder of $\frac{a}{m}$ and *then* apply the algorithm.

```
def modular_exponentiatior(a,n,m)
  """ modular exponentiator takes in three arguments: an base, a, an exponent, n, and a modulus,
      m.  Then, it returns a**n modulo m.
  """
  if n == 0:
    return 1
  else:
    if n % 2 == 0:
      return (((modular_exponentiator(a,n/2,m))^2)%m)
    elif n % 2 == 1:
      return ((a*(modular_exponentiator(a,n-1,m)))%m)
```

Let's run through an example. Consider $a^{100} \bmod m$. We have,

$$\begin{aligned} a^{100} &\equiv_m (a^{50} \bmod m)^2 \bmod m \\ &\equiv_m \left(((a^{25} \bmod m)^2 \bmod m)^2 \bmod m \right) \\ &\equiv_m \left(\left((a(a^{24} \bmod m)^2 \bmod m)^2 \bmod m \right) \right) \\ &\equiv_m \left(\left(\left(((a(a^{12} \bmod m)^2) \bmod m)^2 \bmod m \right) \right) \right) \end{aligned}$$

Etc. So how does it do in terms of efficiency? Well, if μ is the number of bits in the binary representation of μ, and ν is the number of binary bits of n, then we have

$$\mu = \log_2(m+1) \text{ and } \nu \leq \log_2(n+1)$$

The total number of operations, then, will be $2\nu\mu^2$, so the time to execute scales somewhat logarithmically with the size of the argument. Pretty good!

Wilson's theorem has a converse that always holds. However, Fermat's Theorem fails for what are called **Carmichael numbers**, which are numbers satisfying Fermat's Theorem that are not primes. We know a few things about Carmichael numbers: first, the smallest one is 561, and second, there are infinitely many of them. The upper bound formula is a little, uh, opaque, so we'll just toss out a nice, simple lower bound formula. Let $C(n)$ denote the number of Carmichael numbers less than n. Then,

$$C(n) > n^{\frac{2}{7}}$$

Most things involving Carmichael numbers are a little beyond the scope of this course, so let's just prove that 561 is a Carmichael number, i.e. $\forall a \perp 561$, $a^{560} \equiv_{561} 1$.

Proof. Suppose that $a \perp 561$. Then, a is relatively prime to each of the factors of 561 ($a \perp 3, a \perp 11, a \perp 17$). So, by Fermat's Theorem, $a^2 \equiv_3 1$, $a^{10} \equiv_1 11$, and $a^{16} \equiv_{17} 1$. We can exponentiate these modular congruences. For each of the a^{p-1}'s, we raise them to $\frac{560}{p-1}$ to obtain a^{560}. Thus, we have

$$a^{2\times 280} \equiv_3 1 \qquad a^{56\times 10} \equiv_{11} 1 \qquad a^{16\times 35} \equiv_{17} 1$$

Therefore, by the Chinese Remainder Theorem, $a^{560} \equiv_{561} 1$. ■

5.3 Tests for Primality

The computation of $a^m \bmod n$ can be used to "test" an odd number $n \geq 3$ for primality in an efficient manner. The reasoning behind the scare quotes around "test" will become apparent later. To test n for primality using a, where $2 \leq a \leq n-1$, we

1. first check that a is relatively prime to n.
2. If it is not, then $gcd(a, n) \geq 2$ is a divisor of n, so n is composite. Because n is odd, then $n-1$ must be even, so we can write $n-1 = t\cdot 2^s$ for $s \geq 1$. If t is odd, then AAAAAAAAAAAAAAAAAAAAAAAAAAA finish later

6 Euler's Function and Euler's Theorem

6.1 The φ function

For $m \geq 1$, we define the Euler φ function as

$$\varphi(m) = |\{i : 0 \leq i \leq n-1 \text{ and } i \perp m\} \tag{14}$$

If we think of m as being a modulus, then we can think of the φ function as returning the number of equivalence classes mod m for which a multiplicative inverse exists. Therefore, if we let $\mathbb{Z}_m^*$ denote the set given in (14), then

$$\mathbb{Z}_m^* \subseteq \mathbb{Z}_m$$

Recall that $\mathbb{Z}_m$ was closed under addition and multiplication, etc. The same is not necessarily true for $\mathbb{Z}_m^*$.

6.1.1 Formula and Properties

We want some formula such that, given $x \in \mathbb{Z}$, we can find $\varphi(x)$. First, let's examine the case of the primes. Well, for a prime p, φ will return the number of integers between 0 and $p-1$ inclusive that are relatively prime to p. But, because p is prime, then it it is relatively prime to all $1 \leq p \leq p-1$. So, $\varphi(p) = p-1$.

What about $\varphi(p^\mu)$? Well, which elements between 0 and p^μ are not relatively prime to p? Every p'th one. So, we have

$$\begin{aligned}\varphi(p^\mu) &= p^\mu - \frac{p^\mu}{p} \\ &= p^\mu\left(1 - \frac{1}{p}\right)\end{aligned}$$

We're getting closer—now, we just need to find a way of obtaining $\varphi(x)$ if the argument x is a product of multiple pairwise relatively prime factors.

Theorem 6.1. *The φ function is multiplicative over relatively prime arguments. I.e., if $n \perp m$, then*

$$\varphi(nm) = \varphi(n)\varphi(m)$$

Proof. If $m \geq 1$ and $l \geq 1$ are relatively prime, the Chinese Remainder Theorem says there is a one-to-one correspondence between pairs $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_l$ and $x \in \mathbb{Z}_{ml}$.

$$\mathbb{Z}_{nm} \overset{1:1}{\longleftrightarrow} \mathbb{Z}_n \times \mathbb{Z}_m \tag{15}$$

On the homework, we showed that $(a \perp n) \wedge (a \perp m) \iff a \perp nm$, so (15) is one-to-one between $\mathbb{Z}_m^* \times \mathbb{Z}_l^*$ and the elements of $\mathbb{Z}_{ml}^*$. Thus,

$$\varphi(m)\varphi(l) = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_l^*| = |\mathbb{Z}_{ml}^*| = \varphi(ml)$$

■

Now, we seek to generalize to a composite number m. Recall that we can express m as a factorization of primes $p_1, p_2, \ldots, p_k, \ldots$ where the prime p_i has multiplicity μ_{p_i}. That is, we can express m by the prime factorization

$$m = 2^{\mu_2} \cdot 3^{\mu_3} \cdots p^{\mu_p} \cdots$$

Where $\mu \geq 0$ for only finitely many p_i. We shall write this as

$$m = \prod_{p|m} p^{\mu_p}$$

Where p runs through the primes dividing m, that is, the primes p for which $\mu_p \geq 1$. Then, we have

$$\begin{aligned}\varphi(m) &= \prod_{p|m} \varphi(p^{\mu_p}) \\ &= \prod_{p|m} p^{\mu_p}\left(1 - \frac{1}{p}\right) \\ &= m \prod_{p|m}\left(1 - \frac{1}{p}\right)\end{aligned}$$

Note that this formula gives values of $\varphi(m)$, but requires knowledge of the prime factoriztion of m. Interestingly, the ratio of $\varphi(m)$ to m depends only on *which* primes divide m (i.e., the *set* of prime divisors of m), not on how many times each prime divides m (i.e., the multiset of prime divisors of m). Armed with a better understanding of the φ function, we can go on to prove an interesting theorem.

6.2 Euler's Theorem

Theorem 6.2 (Euler's Theorem)**.** *Suppose we have some $m \geq 1$ and $a \perp m$. Then,*

$$a^{\varphi(m)} \equiv_m 1$$

We can see this is a generalization of Fermat's Theorem—if $m = p$ (where p is a prime), then $\varphi(p) = p - 1$, so we have

$$a^{p-1} \equiv_p 1$$

Proof. Let $I = \{0 \leq i \leq m - 1 : i \perp m\}$, so that $|I| = \varphi(m)$. Then, consider a function $f : I \to I$ given by

$$f(i) = ai \bmod m$$

We are given in the statement that $a \perp m$, so therefore a has a multiplicative inverse, $a^{-1} \bmod m$. Thus, the function f is invertible, and so must be a permutation of the elements of I. Then, we have

$$\prod_{i \in I} f(i) \equiv_m \prod_{i \in I} (ai)$$

Because $f(i)$ is a permutation, then the right hand side is the same as the product of the elements in I in a different order. But, multiplication is commutative, so we have

$$\prod_{i \in I} f(i) \equiv_m \prod_{i \in I} i$$

$$a^{\varphi(m)} \cancel{\prod_{i \in I} i}^{1} \equiv_m \cancel{\prod_{i \in I} i}^{1}$$

$$a^{\varphi(m)} \equiv_m 1$$

■