

b is a multiple of a
 a is a divisor of b

$$a \mid b \stackrel{\text{def}}{\iff} a \cdot q = b \quad \left\{ \begin{array}{l} a \text{ divides } b \\ b \text{ is a multiple of } a \end{array} \right.$$

18.7.2023

$$a, m \in \mathbb{Z} \Rightarrow \exists b, q: a = mq + b \quad b < m$$

$$a \equiv b \pmod{m} \iff \begin{array}{l} m \mid a - b \\ m \cdot q = a - b \\ a = b + m \cdot q \\ b = a - m \cdot q \end{array}$$

$$\frac{a \mid b \Rightarrow a \mid b \cdot c}{a \mid b \Rightarrow a \mid b \cdot c}$$



$$\begin{array}{l} a \equiv b \pmod{m} \Rightarrow \\ a \pm c \equiv b \pm c \pmod{m} \\ a \cdot c \equiv b \cdot c \pmod{m} \\ ac \equiv bc \pmod{m \cdot c} \end{array}$$

Any multiple

$$M = \{ m \cdot d \mid m \in \mathbb{Z} \}$$



Euclid

$$\left\{ \begin{array}{l} \text{smallest } m \\ \{ ax + by \mid x, y \in \mathbb{Z} \} \\ = \{ m \cdot d \mid m \in \mathbb{Z} \} \end{array} \right.$$



extended Euclid

Bézout:

$$ax + by = c \text{ solvable} \iff (a, b) \mid c$$



Euclid's lemma

$$\left\{ \begin{array}{l} (a, b) = 1 \\ (a, c) = 1 \\ c \mid a \cdot b \end{array} \right\} \Rightarrow c \mid b$$

$(a, b) = 1 \Rightarrow a \mid b \mid c$



Unique decomposition of integers

$$\left\{ \begin{array}{l} ax = 1 \pmod{m} \\ (a, m) = 1 \end{array} \right\} \Rightarrow x = a^{-1} \rightarrow \begin{array}{c} \mathbb{F}_p \\ \uparrow \\ m \mid a \\ \text{field} \end{array}$$

$$\begin{array}{l} ac \equiv bc \pmod{m} \Rightarrow \\ a \equiv b \pmod{\frac{m}{(a, m)}} \end{array}$$

Chinese Remainder

$$\left\{ \begin{array}{l} a \cdot b \equiv 0 \pmod{m} \\ (a, m) = 1 \\ b \equiv 0 \pmod{m} \end{array} \right\} \Rightarrow \begin{array}{l} c \equiv 0 \pmod{a} \\ c \equiv 0 \pmod{b} \\ \Rightarrow c \equiv 0 \pmod{a \cdot b} \end{array}$$



little Fermat, Euler's Theorem

$$aA \equiv A$$

Chinese Remainder

$$\begin{array}{l} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{array}$$

Chinese Remainder

$$N = \prod m_i$$

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_2 \pmod{m_2}$$

has a unique solution, if

$$(m_i, m_j) = 1 \quad (i \neq j)$$

Proof:

① solution is unique
(Euler 2)

$$x - y \equiv 0 \pmod{m_1}$$

$$x - y \equiv 0 \pmod{m_2}$$

$$\Rightarrow x - y \equiv 0 \pmod{m_1 \cdot m_2}$$

② $(m_1, m_2) = 1$
 $x \equiv a_1 \pmod{m_1}$
 $x \equiv a_2 \pmod{m_2}$

$$q_1 m_1 + q_2 m_2 = 1$$

Bézout
(~~and~~ Euclid)

$$q_2 m_2 = 1 - q_1 m_1$$

$$a_{12} = a_1 q_2 m_2 + a_2 q_1 m_1$$

$$\dots =$$

$$= a_1 + (a_2 - a_1) \cdot q_1 \cdot m_1 \equiv a_1 \pmod{m_1}$$

$$\text{or } \mathbb{Z}/N \cong \mathbb{Z}/m_1 \times \dots \times \mathbb{Z}/m_k$$

$$a_{12} \equiv a_1 \pmod{m_1}$$

$$a_{12} \equiv a_2 \pmod{m_2}$$

~~$$a_{12} \equiv a_1$$~~

$$x \equiv a_{12} \pmod{m_1 \cdot m_2}$$

$$x \equiv a_3 \pmod{m_3}$$

x

$$a_{12}$$

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x = a_1 \pmod{m_1}$$

$$x = a_2 \pmod{m_2}$$

$$(m_1, m_2) = 1$$

$$\Rightarrow \exists q_1, q_2 \quad q_1 m_1 + q_2 m_2 = 1$$

$$\Rightarrow a_1 q_1 m_1 + a_1 q_2 m_2 = a_1$$

$$\Rightarrow a_1 q_2 m_2 = a_1 (1 - q_1 m_1)$$

compute q_1, q_2 by extended euclid, then

$$a_{12} = x := a_1 q_2 m_2 + a_2 q_1 m_1 = F(a_1, a_2, m_1, m_2)$$

$$= a_1 (1 - q_1 m_1) + a_2 q_1 m_1$$

$$= a_1 + (a_2 - a_1) q_1 m_1 \equiv a_1 \pmod{m_1}$$

$$\begin{aligned} 3 \mid x &\Rightarrow x = 3q_1 \\ 7 \mid x &\Rightarrow x = 7q_2 \end{aligned}$$

$$\} \Rightarrow x = 21q_3$$

else

$$x \equiv a_{12} \pmod{m_1}$$

$$x \equiv a_{12} \pmod{m_2}$$

~~$$x \equiv a_1$$~~

$$x \equiv a_{12} \pmod{m_1 \cdot m_2}$$

$$x \equiv a_3 \pmod{m_3}$$

in room 1
 in room 2
 in room 3
 in room 4
 in room 5
 in room 6
 in room 7
 in room 8
 in room 9
 in room 10
 in room 11
 in room 12
 in room 13
 in room 14
 in room 15
 in room 16
 in room 17
 in room 18
 in room 19
 in room 20
 in room 21
 in room 22
 in room 23
 in room 24
 in room 25
 in room 26
 in room 27
 in room 28
 in room 29
 in room 30
 in room 31
 in room 32
 in room 33
 in room 34
 in room 35
 in room 36
 in room 37
 in room 38
 in room 39
 in room 40
 in room 41
 in room 42
 in room 43
 in room 44
 in room 45
 in room 46
 in room 47
 in room 48
 in room 49
 in room 50
 in room 51
 in room 52
 in room 53
 in room 54
 in room 55
 in room 56
 in room 57
 in room 58
 in room 59
 in room 60
 in room 61
 in room 62
 in room 63
 in room 64
 in room 65
 in room 66
 in room 67
 in room 68
 in room 69
 in room 70
 in room 71
 in room 72
 in room 73
 in room 74
 in room 75
 in room 76
 in room 77
 in room 78
 in room 79
 in room 80
 in room 81
 in room 82
 in room 83
 in room 84
 in room 85
 in room 86
 in room 87
 in room 88
 in room 89
 in room 90
 in room 91
 in room 92
 in room 93
 in room 94
 in room 95
 in room 96
 in room 97
 in room 98
 in room 99
 in room 100

\bar{x} \bar{y}
 μ μ
 x x

12/19/2019

Page

$$\begin{array}{c} \nearrow \\ \text{III} \\ \text{---} \\ \nearrow \\ \text{X} \end{array}$$

7

GOESLINGER, J. 219 OWIN

~~1~~

$\begin{matrix} 2 \\ \equiv \\ \times \end{matrix}$
 $\begin{matrix} 4 \\ \equiv \\ \times \end{matrix}$
 $\begin{matrix} 8 \\ \equiv \\ \times \end{matrix}$

$$\begin{array}{cc} \uparrow & \uparrow \\ (5, 4) & (0, 4) \end{array}$$

$$1 + 9 = 13 \quad \text{mod } 15$$

$$4.9 \geq (1.0, 4.04)$$

[illegible]

Beispiel 1

Euler 1

$$(a, c) = 1 \Rightarrow c \mid b$$

$$ax + by = 1 \Rightarrow (ax + by)(c) = c \Rightarrow ax + by = \frac{c}{c} = 1$$

$$ax + by = 1$$

$$ax + by = 1 \Rightarrow (ax + by) \cdot c = c \Rightarrow ax + by = \frac{c}{c} = 1$$

$$a \cdot b \equiv 0 \pmod{c}$$

$$(a, c) = 1$$

Euler 2

$$(a, b) = 1 \Rightarrow a \mid c, b \mid c \Rightarrow a \cdot b \mid c$$

$$a \equiv 0 \pmod{c}$$

$$(a, b) = 1$$

$$c \equiv 0 \pmod{a}$$

$$c \equiv 0 \pmod{b}$$

$$\Rightarrow a \cdot b \mid c$$

$$\Rightarrow a \cdot b \mid c \Rightarrow \frac{c}{a \cdot b} = 1$$

$$\Rightarrow ax + by = 1$$

$$\Rightarrow c \mid b$$

(1) Each multiple m of integer looks like

$$m = \{ n \cdot a \mid n \in \mathbb{Z} \}, \quad a = \text{smallest integer of } n$$

(2) $m = \{ ax + by \mid x, y \in \mathbb{Z} \}$

$$\Rightarrow ax + by = c$$

$$= \{ n \cdot (a, b) \mid n \in \mathbb{Z} \}$$

= smallest multiple containing a and b

has an integer solution \Leftrightarrow

$$(a, b) \mid c$$

(3) Euler's Lemma

\neg clerk system

$$\Rightarrow ax + cy = 1$$

$$\Rightarrow b = b(ax + cy)$$

$$= abx + cby$$

$$= \left(\frac{b}{c} x + by \right) \cdot c \Rightarrow c \mid b$$

$$c \mid a \cdot b \Rightarrow c \mid a \text{ or } c \mid b$$

(4) Congruences

$$a \equiv 0 \pmod{m} \Leftrightarrow m \mid a \Leftrightarrow a = x \cdot m$$

$$\left. \begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array} \right\} \Rightarrow a \pm c \equiv b \pm d \pmod{m}$$

$$a \not\equiv 0 \pmod{m} \Rightarrow b \not\equiv 0 \pmod{m}$$

$$ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{\frac{m}{(c, m)}}$$

$$(c, m) = 1 : a \equiv b \pmod{m} \quad \begin{array}{l} \equiv b \pmod{m} \text{ if } (c, m) = 1 \\ \text{if } (c, m) = 1, \text{ you can divide} \end{array}$$

$$b = 0 : a \equiv 0 \pmod{m}$$

and: $a \cdot b \equiv 0 \pmod{m}$
 $\Rightarrow a \equiv 0 \pmod{m} \text{ or } b \equiv 0 \pmod{m}$

⑤ Fermat's little theorem

$$a^{p-1} \equiv 1 \pmod{p}$$

$$A = \{1, 2, \dots, p-1\} \quad a \cdot A = \{a, 2a, \dots, a \cdot (p-1)\}$$

$A = a \cdot A$ because all elements of A are distinct:

$$\left(\begin{array}{l} a x_i \equiv a x_j \pmod{p} \\ \Rightarrow x_i = x_j \pmod{p} \end{array} \right)$$

$$\Rightarrow \prod_{i=1}^{p-1} x_i = a \cdot \prod_{i=1}^{p-1} x_i$$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

Euler's + theorem

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

$$\text{if } (a, m) = 1$$

Proof as above with $A = \{x_1, x_2, \dots, x_{\phi(m)}\}$

a reduced residue system mod m

$$(x_i, m) = 1 \quad (\text{all } i)$$

$$x_i \not\equiv x_j \pmod{m} \quad (i \neq j)$$

Every positive integer has a unique composition into prime factors

$$p_1^{a_1} \mid \prod p_i^{x_i} = p_1^{a_1} \mid \prod q_j^{y_j}$$

$$\Rightarrow p_i = q_i, x_i = y_i$$

$$\textcircled{c} p_i = q_i$$

(if correctly ordered)

$$\text{because: } p_i \neq q_j \text{ (call } j)$$

$$p \mid \prod q_j$$

$$\Rightarrow p \mid q_j$$

$$\Rightarrow p = q_j \text{ (at least one } q_j)$$

$$\Rightarrow p = q_j$$

$$\textcircled{b} p_1 \mid \prod p_i^{a_i}$$

$$\Rightarrow p_1 = q_j$$

$$\left. \begin{aligned} a &= m_a \cdot d \\ b &= m_b \cdot d \end{aligned} \right\} \Rightarrow$$

any module containing a and b contains d
the smallest module as generated by the greatest c.d.

Kundennummer: 123 456 789
Rechnungsnummer: 123 456 789

$$p_1^{a_1} \mid p_1^{b_1}$$

prime

$$\Rightarrow a_1 = b_1, p_1 = q_1$$

Ihre detaillierte Rechnung für April 2010

Empfänger: Empfänger
Datum: 12.04.10
Seite: 1 von 1

①

Each module M (of integers) looks like

$$M = \{m \cdot d \mid m \in \mathbb{Z}\}$$

with $d =$ smallest integer in M

Remark: Assume $x \in M$ with

$$m \cdot d < x < (m+1) \cdot d$$

$$\Rightarrow 0 < y = x - m \cdot d < d$$

y integer, $y < d$

$$M = \{ax + by \mid x, y \in \mathbb{Z}\} = \{m \cdot d \mid m \in \mathbb{Z}\}$$

$$d = (a, b)$$

②

The equation

$$ax + by = c$$

has integer solutions ~~only~~ iff

$$(a, b) \mid c$$

$M = \{ax + by \mid x, y \in \mathbb{Z}\}$ is a module

$$\Rightarrow M = \{m \cdot d \mid m \in \mathbb{Z}\}, \text{ ~~at least~~ } d = (a, b)$$

$$\Rightarrow c = d \cdot m$$

$$A \Rightarrow B$$

$$M \text{ module} \Rightarrow M = \{m \cdot d\}$$

$$\text{Proof: } \exists d \in M, +$$

$$\forall x \in M, \exists d \leq x$$

$$\wedge M = \{m \cdot d \mid -\}$$

$$A \Rightarrow B$$

$$M \text{ module } \wedge$$

$$d = \min \{x \in M \mid x > 0\}$$

$$\Rightarrow M = \{m \cdot d \mid -\} \mid B$$

$$\neg B \Rightarrow \neg A = \neg A_1 \vee \neg A_2$$

$$A \Rightarrow \neg A_2$$

$$d \mid c \quad (a, b) \mid c$$

④

If $c|ab$ and $(c,a)=1$ then $c|b$

$$\left. \begin{array}{l} c|a \cdot b \\ (c,a)=1 \end{array} \right\} \Rightarrow c|b$$

Euler's Lemma

$$\begin{aligned} ax + by &= 1 \Rightarrow b = b(ax + cy) \\ &= abx + c \cdot by \\ &= \underbrace{\left(\frac{ab}{c} x + by \right)}_{\text{integers}} \cdot c \end{aligned}$$

then
 $c|a \cdot b$
 $c|a$ or $c|b$

$$\begin{aligned} ax + by &= n \cdot cd \\ a &= m_1 \cdot d \\ b &= m_2 \cdot d \end{aligned}$$

⑤

Congruences

$$\begin{aligned}
 a &\equiv 0 \pmod m \iff m \mid a \\
 a &\equiv b \pmod m \iff a \pm c \equiv b \pm c \pmod m \\
 c &\equiv d \pmod m \iff a \cdot c \equiv a \cdot d \pmod m \\
 a \cdot c &\equiv b \cdot c \pmod m \implies a \equiv b \pmod{\frac{m}{(c,m)}}
 \end{aligned}$$

$$\begin{aligned}
 b &= 0 \\
 a &\equiv 0 \pmod b
 \end{aligned}$$

$$a \equiv b \pmod m \iff (c,m) = 1$$

because: $(c,m) = 1$

$$a - b = 0 \pmod m$$

$$\begin{aligned}
 &\iff m \mid a - b \\
 &\iff a - b = 0 \pmod m \text{ or } b = 0 \pmod m
 \end{aligned}$$

$$m \mid (a-b) \cdot c$$

$$\frac{m}{d} \mid (a-b) \cdot \frac{c}{d}$$

$$\left(\frac{m}{d}, \frac{c}{d} \right) = 1$$

$$\frac{m}{d} \mid a - b$$

$$a - b \equiv 0 \pmod{\frac{m}{d}}$$

⑥ Linear Congruences

$$ax \equiv b \pmod{m}$$

$$\Leftrightarrow ax - b \equiv 0 \pmod{m}$$

$$\Leftrightarrow m \mid (ax - b)$$

$$\Leftrightarrow \text{exists } k$$

$$m \cdot k = ax - b$$

$$ax - m \cdot k = b$$

solvable iff $\gcd(a, m) \mid b$

$$x \equiv \frac{b}{a} \pmod{\frac{m}{\gcd(a, m)}}$$

$$ax \equiv b \pmod{m}$$

$$\text{with } (a, m) = 1$$

$\Rightarrow \mathbb{Z}_p$ is a field (unique inverse)

$$(a, m) = 1$$

$$ax \equiv b \pmod{m}$$

has exactly one solution

because: let $x_i = 0, 1, \dots, m-1$

$$y \equiv ax \pmod{m}$$

$$ax_i \equiv ax_j \pmod{m}$$

$$a(x_i - x_j) \equiv 0 \pmod{m}$$

$$m \mid a(x_i - x_j)$$

$$a(x_i - x_j) \equiv 0 \pmod{m}$$

$$x_i, x_j < m$$

$$x_i = x_j$$

$$\{a \mid a \equiv 0 \pmod{m}\} =$$

$$\{x \mid x \equiv 0 \pmod{m}\}$$

$$a \neq 0 \pmod{m} \Rightarrow x_i - x_j = 0$$

[illegible]

$$\begin{aligned} \sum_{i=1}^n x_i &= \sum_{i=1}^n x_i' \\ \sum_{i=1}^n x_i &= \sum_{i=1}^n x_i' \end{aligned}$$

[illegible]

1-2
1-3
1-4
1-5
1-6
1-7
1-8
1-9
1-10
1-11
1-12
1-13
1-14
1-15
1-16
1-17
1-18
1-19
1-20
1-21
1-22
1-23
1-24
1-25
1-26
1-27
1-28
1-29
1-30
1-31
1-32
1-33
1-34
1-35
1-36
1-37
1-38
1-39
1-40
1-41
1-42
1-43
1-44
1-45
1-46
1-47
1-48
1-49
1-50
1-51
1-52
1-53
1-54
1-55
1-56
1-57
1-58
1-59
1-60
1-61
1-62
1-63
1-64
1-65
1-66
1-67
1-68
1-69
1-70
1-71
1-72
1-73
1-74
1-75
1-76
1-77
1-78
1-79
1-80
1-81
1-82
1-83
1-84
1-85
1-86
1-87
1-88
1-89
1-90
1-91
1-92
1-93
1-94
1-95
1-96
1-97
1-98
1-99
1-100
1-101
1-102
1-103
1-104
1-105
1-106
1-107
1-108
1-109
1-110
1-111
1-112
1-113
1-114
1-115
1-116
1-117
1-118
1-119
1-120
1-121
1-122
1-123
1-124
1-125
1-126
1-127
1-128
1-129
1-130
1-131
1-132
1-133
1-134
1-135
1-136
1-137
1-138
1-139
1-140
1-141
1-142
1-143
1-144
1-145
1-146
1-147
1-148
1-149
1-150
1-151
1-152
1-153
1-154
1-155
1-156
1-157
1-158
1-159
1-160
1-161
1-162
1-163
1-164
1-165
1-166
1-167
1-168
1-169
1-170
1-171
1-172
1-173
1-174
1-175
1-176
1-177
1-178
1-179
1-180
1-181
1-182
1-183
1-184
1-185
1-186
1-187
1-188
1-189
1-190
1-191
1-192
1-193
1-194
1-195
1-196
1-197
1-198
1-199
1-200
1-201
1-202
1-203
1-204
1-205
1-206
1-207
1-208
1-209
1-210
1-211
1-212
1-213
1-214
1-215
1-216
1-217
1-218
1-219
1-220
1-221
1-222
1-223
1-224
1-225
1-226
1-227
1-228
1-229
1-230
1-231
1-232
1-233
1-234
1-235
1-236
1-237
1-238
1-239
1-240
1-241
1-242
1-243
1-244
1-245
1-246
1-247
1-248
1-249
1-250
1-251
1-252
1-253
1-254
1-255
1-256
1-257
1-258
1-259
1-260
1-261
1-262
1-263
1-264
1-265
1-266
1-267
1-268
1-269
1-270
1-271
1-272
1-273
1-274
1-275
1-276
1-277
1-278
1-279
1-280
1-281
1-282
1-283
1-284
1-285
1-286
1-287
1-288
1-289
1-290
1-291
1-292
1-293
1-294
1-295
1-296
1-297
1-298
1-299
1-300
1-301
1-302
1-303
1-304
1-305
1-306
1-307
1-308
1-309
1-310
1-311
1-312
1-313
1-314
1-315
1-316
1-317
1-318
1-319
1-320
1-321
1-322
1-323
1-324
1-325
1-326
1-327
1-328
1-329
1-330
1-331
1-332
1-333
1-334
1-335
1-336
1-337
1-338
1-339
1-340
1-341
1-342
1-343
1-344
1-345
1-346
1-347
1-348
1-349
1-350
1-351
1-352
1-353
1-354
1-355
1-356
1-357
1-358
1-359
1-360
1-361
1-362
1-363
1-364
1-365
1-366
1-367
1-368
1-369
1-370
1-371
1-372
1-373
1-374
1-375
1-376
1-377
1-378
1-379
1-380
1-381
1-382
1-383
1-384
1-385
1-386
1-387
1-388
1-389
1-390
1-391
1-392
1-393
1-394
1-395
1-396
1-397
1-398
1-399
1-400
1-401
1-402
1-403
1-404
1-405
1-406
1-407
1-408
1-409
1-410
1-411
1-412
1-413
1-414
1-415
1-416
1-417
1-418
1-419
1-420
1-421
1-422
1-423
1-424
1-425
1-426
1-427
1-428
1-429
1-430
1-431
1-432
1-433
1-434
1-435
1-436
1-437
1-438
1-439
1-440
1-441
1-442
1-443
1-444
1-445
1-446
1-447
1-448
1-449
1-450
1-451
1-452
1-453
1-454
1-455
1-456
1-457
1-458
1-459
1-460
1-461
1-462
1-463
1-464
1-465
1-466
1-467
1-468
1-469
1-470
1-471
1-472
1-473
1-474
1-475
1-476
1-477
1-478
1-479
1-480
1-481
1-482
1-483
1-484
1-485
1-486
1-487
1-488
1-489
1-490
1-491
1-492
1-493
1-494
1-495
1-496
1-497
1-498
1-499
1-500
1-501
1-502
1-503
1-504
1-505
1-506
1-507
1-508
1-509
1-510
1-511
1-512
1-513
1-514
1-515
1-516
1-517
1-518
1-519
1-520
1-521
1-522
1-523
1-524
1-525
1-526
1-527
1-528
1-529
1-530
1-531
1-532
1-533
1-534
1-535
1-536
1-537
1-538
1-539
1-540
1-541
1-542
1-543
1-544
1-545
1-546
1-547
1-548
1-549
1-550
1-551
1-552
1-553
1-554
1-555
1-556
1-557
1-558
1-559
1-560
1-561
1-562
1-563
1-564
1-565
1-566
1-567
1-568
1-569
1-570
1-571
1-572
1-573
1-574
1-575
1-576
1-577
1-578
1-579
1-580
1-581
1-582
1-583
1-584
1-585
1-586
1-587
1-588
1-589
1-590
1-591
1-592
1-593
1-594
1-595
1-596
1-597
1-598
1-599
1-600
1-601

$\in M \Rightarrow$
 $-a \mid r_{n-2}$
 $-a \mid b$
 $-a \mid a$
 $\Rightarrow d =$

$$\begin{aligned} & \tau_i \in M \Rightarrow 0 \\ & \left. \begin{array}{l} \tau_{n-1} \\ \vdots \\ \tau_n \\ \tau_n \end{array} \right\} \tau_{n-2} \end{aligned}$$
$$a \leq r_{n-1}$$

Extended Euclid

① $(a, m) = 1$ then:

$ax + my = 1$ is solvable

$\Leftrightarrow ax \equiv 1 \pmod{m}$ is solvable

② $a \cdot b \equiv 0 \pmod{m}$ \Rightarrow
 $(a, m) = (b, m) = 1$

$a \equiv 0 \pmod{m}$ or

$b \equiv 0 \pmod{m}$

$$r_0 = a, \quad r_1 = b$$

$$s_0 = 1, \quad s_1 = 0$$

$$t_0 = 0, \quad t_1 = 1$$

$$r_{i+1} = r_{i-1} - q_i r_i$$

$$s_{i+1} = s_{i-1} - q_i s_i$$

$$t_{i+1} = t_{i-1} - q_i t_i$$

$$r_{m+1} = 0; \quad [d = \gcd(m)] = (a, b)$$

$$r_n = a s_n + b t_n = 1$$

$$a \cdot s_n \equiv 1 \pmod{b}$$

$$r_0 = a s_0 + b t_0$$

$$r_1 = a s_1 + b t_1$$

$$r_{k+1} = r_{k-1} - q_k r_k$$

$$= (a \cdot s_{k-1} + b t_{k-1}) - q_k (a s_k + b t_k)$$

$$= a (s_{k-1} - q_k s_k) + b (t_{k-1} - q_k t_k)$$

$$= a \cdot s_{k+1} + b \cdot t_{k+1}$$

$$r_2 = r_0 - q_1 r_1$$

$$r_{i+n} = r_i - q_i r_{i+1}$$

$$S_0 = 1, S_1 = 0$$

$$t_0 = 0, t_1 = a$$

$$r_0 = q_1$$

$$r_1 = b$$

$$r_{i+n} = a \cdot S_n + b \cdot t_n$$

$$= r_0 S_n + r_1 t_n$$

$$r_{2+n} = r_{2-n} - q_2 \cdot r_2$$

$$= a \cdot S_{2-n} + b \cdot t_{2-n}$$

$$- q_2 (a S_2 + b t_2)$$

$$= a \cdot (S_{2-n} - q_2 S_2) + b (t_{2-n} - q_2 t_2)$$

$$= a \cdot S_{2+n} + b \cdot t_{2+n}$$

$$r_{n+n} = 0$$

$$r_0 = a \cdot S_0 + b \cdot t_0 = 0$$

$$r_1 = a \cdot S_1 + b \cdot t_1 = 1$$

$$r_{2-n} = a \cdot S_{2-n} + b \cdot t_{2-n}$$

$$r_2 = a \cdot S_2 + b \cdot t_2$$

$d \in M$ smallest ntgs

$x \in M$ not a multiple of d

$$n \cdot d < x < (n+1) \cdot d$$

$$\Rightarrow x - n \cdot d = x - n \cdot d \in M$$
$$= y < d$$
$$\Rightarrow$$

$$0 < x - n \cdot d = y \in M$$

Every ntgs module is generated by its smallest element
ged: what is the smallest module containing a and b ?

$$d = \text{ged}(a, b)$$

$$a = a_1 \cdot d$$

$$b = b_1 \cdot d$$

$$a > b$$

$$a - q \cdot b = r$$

$$a = b \cdot q + r \quad 0 \leq r < b$$

$$r = 0 \Rightarrow a = b \cdot q; \quad b = \text{ged}(a, b)$$

For each module M :

$$M = \{ n \cdot d \mid n \in \mathbb{Z} \}$$

d = smallest ntgs of M

$$0 < y = x - n \cdot d < (n+1) \cdot d - n \cdot d = d$$

Module M :

if $x, y \in M$ then $x - y \in M, x + y \in M$

closed under (addition and) subtraction

redundant

$0 \in M$ (always)

$y \in M \Rightarrow 0 - y = -y \in M$

$x, y \in M \Rightarrow x, -y \in M \Rightarrow x - (-y) = x + y \in M$

$x \in M \Rightarrow n \cdot x$ (all $n \in \mathbb{N}$)

all elements of M are multiples of an integer d ,
the smallest ^{positive} integer of M

Leibniz'sche Division und Rest:

$$(1) \quad a, b \in \mathbb{N} : \exists n, r \in \mathbb{N}_0 :$$

$$a = n \cdot b + r ; \quad r < b$$

Damit ist

$$r = a - n \cdot b$$

$$\text{Beweis: } n := \max \{ x \in \mathbb{N}_0 \mid x \cdot b \leq a \} = \max \{ x \in \mathbb{N}_0 \mid x \leq \frac{a}{b} \}$$

Die Menge $\{ \dots \}$ ist beschränkt und nicht-leer,
hat also ein Maximum. ~~Aufgabe~~ in WZ

$$r = a - n \cdot b \geq 0,$$

$$\Rightarrow a \geq n \cdot b \quad (n+1) \quad \checkmark$$

~~ist~~

$$2 \mid 10 \Rightarrow 2 \cdot 9 = 10$$

② Dies funktioniert auch für $a, b \in \mathbb{Z}$, $b \neq 0$:

$$m = \max \{ x \in \mathbb{Z} \mid x \leq \frac{a}{b} \} = \begin{cases} \max \{ x \in \mathbb{Z} \mid x \cdot b \leq a \} & b > 0 \\ \max \{ x \in \mathbb{Z} \mid x \cdot b \geq a \} & b < 0 \end{cases}$$

$$r = a - m \cdot b.$$

$$\text{Man definiert: } m = a // b, \quad r = a \% b.$$

Beispiel:

$$10 // 7 = 1 \quad 10 \% 7 = 3$$

$$-10 // 7 = -2 \quad -10 \% 7 = 4$$

$$10 // -7 = -2 \quad 10 \% -7 = -4$$

$$-10 // -7 = 1 \quad -10 \% -7 = -3$$

Der Rest hat das Vorzeichen des Nenners b , denn:

$$b > 0: m \cdot b \leq a \Rightarrow r = a - m \cdot b \geq 0$$

$$b < 0: m \cdot b \geq a \Rightarrow r = a - m \cdot b \leq 0$$

Beachte: man kann nicht mit -1 durchmultiplizieren; wegen:

$$\max \{ x \in \mathbb{Z} \mid x \leq \frac{a}{b} \} =$$

$$\max \{ x \in \mathbb{Z} \mid x \leq \frac{-a}{-b} \}$$

