1 Euclid

Claim 1 *Let $a,\ b \in \mathcal{N}$ $a > b$. Then there is a number $0 \leq r < a$ and a number x so that $a = x \cdot b + r$*

Proof. Say that $a > b$. Take $a-b, a-2b, \ldots$. Consider the first time $a - i \cdot b \leq b$. If $a - ib = b$ the theorem is clear. Else $a - ib < b$. it means that $a - (i-1)b < 2b$ and $a - ib < b$. Thus $a - ib = a - (i-1) - b < 2b - b = b$. □

Works for negative numbers as well:
$-42 = 3 \ \ mod\ 15$.
$-42 = -3 \cdot 15 + 3$.

The Euclid algorithm
$gcd(a, b)$

1. if $b = 0$ return a
2. Else return $gcd(b, a \ mod\ b)$

Claim 2 *The Euclid algorithm is correct and runs in time at most $2 \cdot \log_2 a$*

Proof. Correctness We show that $x \mid a$ and $x \mid b$ implies $x \mid r = a \ mod\ b$. And vise-versa. Set $a = qb + r$. Thus $x \mid a - q \cdot b = r$. This implies $x \mid r$ because $x \mid a$ and $x \mid b$. In the other direction if $x \mid b$ and $x \mid r$, then $x \mid q \cdot b + r = a$.

Running time: The running time will be $O(\log a)$. To show that, we show that every two steps the larger number becomes at most $1/2$ the original one.

To show that first assume that $b < a/2$. After $gcd(a, b)$ we go to $gcd(b, a \ mod\ b)$ and after one iteration the maximum is halved.

Now assume that $b > a/2$. After two iterations the largest number becomes $a \ mod\ b = a - b < a/2$. Thus takes at most $2 \log_2 a$. □

The real answer is log to the base of golden ratio of a.

Theorem 1 *Using the Eucledian algorithm in reverse gives $y, z \in \mathcal{Z}$ so that $y \cdot a + z \cdot b = gcd(a, b)$.*

Proof. Omitted. □

Theorem 2 *Let $a > b \geq 0$. Then $d = gcd(a, b)$ is the smallest positive integer in the infinite set: $Z_{a,b} = \{x \cdot a + y \cdot b \mid x, y \in \mathcal{Z}\}$*

Proof. Let d be the smallest positive number in $Z_{a,b}$. Thus $d = x \cdot a + y \cdot b$. Let $r = gcd(a, b)$ and assume for the sake of contradiction that $r < d$. By Theorem 1, $r \in Z_{a,b}$. This is a contradiction. □

Claim 3 *If $gcd(a, n) = 1$ then there exists z so that $z \cdot a = 1 \ mod\ n$. Namely, a has an* inverse *under modulo n.*

Proof. By Theorem 2, we can find y, z so that $y \cdot n + z \cdot a = gcd(a, n) = 1$ Thus $z \cdot a = 1 \ mod\ n$. □

From now on all computation will be modulo n. Thus, usually I omit the *mod* n.

2 Groups and subgroups

Definition 3 A group: *This needs S and some operation $\oplus$ so that:*

1. *$a \in S$, $b \in S$ implies $a \oplus b \in S$.*
2. *There exists a number e called the units such that:*
3. *Everybody has an inverse. Namely for every $a \in S$ there exist $b \in S$ so that $a \oplus b = e$.*

Claim 4 *Consider $Z_n^* = \{1 \leq x < n \mid gcd(n, x) = 1\}$. Let $\oplus$ be multiplication modulo n. Then Z_n^* is a group.*

Proof. If $gcd(a, n) = gcd(b, n) = 1$, then $gcd(a \cdot b, n) = 1$ because every prime that divides a and every primed that divides b does not belong to the list of primes that divide n. Thus Rule 1 applies. Rule 3 follows from Claim 3. □

Example: $Z_{12}^* = \{1, 5, 7, 11\}$. The operation is a multiplication modulo 12.
$11 \cdot 11 = 1$ *mod* 12 This is because $11 = -1$ *mod* 12 and $-1 \cdot -1$ *mod* 12 $= 1$
The inverse of 7 is 7 itself. $7 \cdot 7 = 1$ *mod* 12.
The inverse of 5 is 5.
$5 \cdot 5 = 1$ *mod* 12
Remark: for a prime p, $Z_p^* = 1, \ldots, p-1$ is a special group. For example: it is known to always be generated by some element r. Namely there exists an $r \in Z_p^*$ so that for every $a \in Z_p^*$ there exists some i so that $r^i = a$.

Theorem 4 Lagrange's theorem *If $S, \oplus$ is a finite group and $S', \oplus$ is a group as well then $|S'|$ divides $|S|$.*

Proof. Omitted (quite hard). □

Infinite group, one example: *Invertible matrices*. Matrices with $det(A) \neq 0$. As $det(A \cdot B) = det(A) \cdot det(B) \neq 0$, Property 1 holds. Let I be the Matrix with 1 in the diagonal and 0 elsewhere. This is our e namely the "one" of the group.

Theorem 5 *If $det(A) \neq 0$ there exists a B so that $B \cdot A = A \cdot B = I$.*

Thus an *infinite* group.

3 Solving $ax = b$ *mod* n

In this section every multiplication and addition of integers is done modulo n. This we do not put modulo n everywhere.

Definition 6 *For an integer a let $G_a = \{a, 2a, 3a \ldots\}$*

Solving $ax = b \ mod \ n$

Let $d = gcd(a, n)$ then:

Claim 5 $G_a = G_d$

Proof. We first show $d \in G_a$. Let y, z so that $y \cdot a + z \cdot n = d$. Since everything is done modulo n, $d \in G_a$.

Thus $d = i \cdot a \ mod \ n$ This means that for every j, $d \cdot j = j \cdot i \cdot a \in G_a$ and so $G_d \subseteq G_a$.

We now show that $G_a \subseteq G_d$. Consider an arbitrary number $m \in G_a$. Namely $m = x \cdot a$ (recall everything is mod n). This means $m - (x \cdot a) = j \cdot n$ for some j. Thus $m = x \cdot a + j \cdot n$. By definition $d \mid a$ and $d \mid n$. Therefore the above number belongs to G_d. □

Corollary 7 *There is a solution to $a \cdot x = b$ only if $d \mid b$.*

Let $d = gcd(a, n)$. and say that $d = x' \cdot a + y' \cdot n$.

Claim 6 *If $d \mid b$ then $ax = b \ (mod \ n)$ has d solutions.*

Proof. Too annoying □

Claim 7 $x_0 = x' \cdot b \cdot d^{-1}$ *is a solution to $ax = b \ mod \ n$.*

Proof. $ax_0 = ax' \cdot b \cdot d^{-1}$.

Note that $a \cdot x' = d \ mod \ n$. So we get $b \cdot d \cdot d^{-1} = b$. □

Claim 8 *All solutions to $ax = b$ are $a(x_0 + i \cdot n \cdot d^{-1})$ for $i = 0, 1, \ldots, d - 1$.*

Proof. $a(x_0 + i \cdot n \cdot d^{-1}) = b + a \cdot i \cdot n \cdot d^{-}1 = b \ mod \ n$. Since all these numbers are different, by Claim 7, these are the solutions for $ax = b \ mod \ n$. □

Theorem 8 a^b *can be computed in $O(\log b)$ operations*

Proof. Omitted □