Integers will be used extensively in crypto

$\mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$

$\underline{b \mid a} \Rightarrow \exists c \in \mathbb{Z}$ s.t. $a = b \cdot c$ (b divides a)

$\underline{b \nmid a} \Rightarrow \neg \exists c \in \mathbb{Z}$ s.t. $a = b \cdot c$ (b divides a)

Thm 1: $\forall a, b, c \in \mathbb{Z}$, we have

i) $a \mid a$, $1 \mid a$, & $a \mid 0$

ii) $0 \mid a$ iff $a = 0$

iii) $a \mid b$ & $a \mid c \Rightarrow a \mid (b + c)$

iv) $a \mid b \Rightarrow a \mid -b$

v) $a \mid b$ & $b \mid c \Rightarrow a \mid c$

Proof of v: $a \mid b \Rightarrow \underline{b = a \cdot d}$ for some d

$b \mid c \Rightarrow c = b \cdot e$ for some e

$\Rightarrow c = (a \cdot d) \cdot e \Rightarrow a \mid c$

rest exercise!

Thm 2: $\forall a, b \in \mathbb{Z}$, $a \mid b$ & $b \mid a \Longleftrightarrow a = \pm b$

Proof: Omitted!

p is prime iff $p > 1$ & only divisible by 1 or p.

Thm 3: Every non-zero integer can be expressed as $n = \pm p_1^{e_1} \cdots p_r^{e_r}$ where the p_i are distinct & e_i are positives. Morever this expression is unique up to a reordering of the primes.

Proof of existence:

If $n=1$, it is obvious

let $n>1$, if n is prime then it is true

if n is composite then

$n = ab$ where $a<n$ & $b<n$

by induction hypothesis both a & b can be written as product of primes. so n could be written as well Δ

proof of uniqueness:

omitted!

Thm 4: For $a, b \in \mathbb{Z}$ with $b>0$ $\exists$ unique $q, r \in \mathbb{Z}$ s-t $a = bq + r$ & $0 \le r < b$

Proof: omitted!

Given $a = bq + r$, we say $a = r \bmod b$

gcd(a,b) is the biggest integer d s.t
$d \mid a$ & $d \mid b$

a & b relatively prime if gcd(a,b) = 1

Thm 5: if gcd(a,b) = d then $\exists\ s,t \in \mathbb{Z}$

such that $as + bt = d$ plus

Proof: omitted !

$a = 12$
$b = 8$
$\gcd(a,b) = 4$
$12 \cdot s + 8t = 4$
$12 \cdot 1 + 8 \cdot -1 = 4$

Thm 6: (1-7 in the book)

For $a, b, c \in \mathbb{Z}$ s.t $c \mid a \cdot b$ & $\gcd(a,c) = 1$
then $c \mid b$

Proof: if gcd(a,c) = 1 using Thm 5.

$\exists\ s,t$ such that $\underline{as + ct = 1}$

$\Rightarrow$ $abs + bct = b$

Since $c \mid \underline{abs}$ (given) & $c \mid bct$

$\Rightarrow$ $c \mid (abs + bct) \Rightarrow c \mid b$ $\square$

Thm 7. (1-9 in the Book)

There are infinetly many primes.

Proof: Assume there are finitely many primes, Let $p_1 \ldots p_k$ are those primes

Let $n = 1 + \prod_{i=1}^{k} p_i$

Let $p \mid n$ (exists due fundemental thm. of arithm.)

p cannot be one of p_i $i \in \{1, \ldots, k\}$ because $n = 1 \bmod p_i$. Contradiction.

$\square$

We say $a \equiv b \bmod n$ if $n \mid (a-b)$

$a \not\equiv b \bmod n$ if $n \nmid (a-b)$

or $a \equiv b \bmod n$ if $a = b + cn$ for some c

some properties of the congrue relation:

1) $a \equiv a \pmod n$

2) $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$

3 $a \equiv b \pmod n$ & $b \equiv c \pmod n$ $\Rightarrow a \equiv c \pmod n$

4) $a \equiv a' \pmod n$ & $b \equiv b' \pmod n$

$\Rightarrow \quad a+b \equiv a'+b' \pmod n$

$\Rightarrow \quad a \cdot b \equiv a' \cdot b' \pmod n$

Proof of 4:

$\underline{a = a' + c_1 n}$ & $\underline{b = b' + c_2 n}$ (Given)

$\underline{a+b = a'+b'} + (c_1+c_2)\, n$

$\Rightarrow \quad n \mid (a+b - (a'+b'))$

$\Rightarrow \quad a+b \equiv a'+b' \pmod n$

similarly for the other part!

Thm-(8) for any odd prime p

if $x^2 \equiv 1 \pmod p \Rightarrow x \equiv 1 \bmod p$
or $x \equiv -1 \bmod p$

Proof: $x^2 \equiv 1 \pmod p$

$\Rightarrow (x-1)(x+1) \equiv 0 \bmod p$

$\Rightarrow p \mid (x-1) \cdot (x+1)$

$\Rightarrow p \mid (x-1)$ or $p \mid (x+1)$ (why?)

$\Rightarrow x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$

LINEAR CONGRUENCES

a^{-1} denotes inverse of a mod n
if $a^{-1} \cdot a = 1 \pmod{n}$ $3 \cdot 2 = 1 \pmod{5}$
$3 \pmod{6}$

Thm 9: $a^{-1} \pmod{n}$ exists iff
$\gcd(a, n) = 1$

Proof: we know that
$\gcd(a,n) = 1$ iff $a \cdot s + nt = 1$
for some (s,t)
note that $a \cdot s \equiv 1 \pmod{n}$ (why?)

Thm 10:
Let $a, n, z, z' \in \mathbb{Z}$ with $n > 0$.
given $d = \gcd(a,n)$ then
$a \cdot z \equiv a \cdot z' \pmod{n}$ iff $z \equiv z' \pmod{\frac{n}{d}}$
$3 \cdot 5 = 3 \cdot 1 \bmod 6$ $5 = 1 \bmod 2$

$\Rightarrow$
$a \cdot z \equiv a \cdot z' \pmod{n} \Rightarrow a \cdot z = a \cdot z' + kn$
$\Rightarrow \frac{a}{d} z = \frac{a}{d} z' + k\frac{n}{d}$
$\frac{a}{d} \cdot z = \frac{a}{d} z' \pmod{\left(\frac{n}{d}\right)}$

$\Longrightarrow$ since $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$

$z = z' \left(\bmod \frac{n}{d}\right)$ (why?)

$\Longleftarrow$

$z \equiv z' \left(\bmod \frac{n}{d}\right) \Rightarrow \frac{a}{d} z \equiv z' \frac{a}{d} \bmod \left(\frac{n}{d}\right)$

$\Rightarrow az \equiv z'a \; (\bmod (n))$ (why?)

Solving Equations of the Form $az = b \pmod n$ for given a, b, n

Thm: (10)

Let $a, b, n \in \mathbb{Z}$ with $n > 0$, and $d = \gcd(a, n)$

If $d \mid b$ then:

$az \equiv b \pmod n$ has a solution, Moreover any z' $z = z' \; (\bmod (n/d))$ is also a solution

If $d \nmid b$ then:

NO SOLUTION

Proof:

If $d \mid b$ then $\frac{a}{d} \cdot z = \frac{b}{d} \mod \left(\frac{n}{d}\right)$

$\Rightarrow z = \left(\frac{a}{d}\right)^{-1} \cdot \frac{b}{d} \left(\mod \frac{n}{d}\right)$ (why ?)

If $d \nmid b$ then

assume $az = b \pmod n$

$\Rightarrow a \cdot z = b + kn \Rightarrow b + kn \equiv 0 \mod d$?

$\Rightarrow b \equiv 0 \pmod d$

contradiction!

CHINESE REMAINDER THM

Let $n_1, \ldots, n_k$ be pairwise relatively prime, positive integers then there exists an integer z such that

$$z \equiv a_i \pmod{n_i} \quad \forall i \in [1 \ldots k]$$

Moreover z' is a solution iff

$$z = z' \pmod n \quad \text{where } n = \prod_{i=1}^{k} n_i$$

3, 5, 7, 11, 17

$z = 2 \mod 3$, $z = 4 \mod 5$ - -

$z \equiv 7 \mod 17$

Proof:

Let $n = \prod_{i=1}^{k} n_i$, $n_i' = n / n_i$

Define $m_i = (n_i')^{-1} \pmod{n_i}$ (why this inverse exists ?)

$w_i = m_i \cdot n_i'$

Note $w_i = 1 \pmod{n_i}$ (why ?)

$w_i = 0 \pmod{n_j}$ $(j \neq i)$ (")

Define $z = \sum_{i=1}^{k} w_i a_i$

$w_i \cdot a_i = a_i \pmod{n_i}$

$w_j \cdot a_j = 0 \pmod{n_i}$

$z \equiv a_i \pmod{n_i}$ (why ?) $\rightarrow$

If $z' \equiv z \pmod{n}$ since $n_i \mid n$

$\Rightarrow z' \equiv z \equiv a_i \pmod{n_i}$

Also assume z' is an another solution

Then clearly $z' \equiv z \pmod{n_i}$ for $1 \le i \le k$

$\Rightarrow n_i \mid (z' - z)$ for $1 \le i \le k$

$\Rightarrow n \mid (z' - z)$ (why ?)

$\Rightarrow z' \equiv z \pmod{n_i}$

Define Z_n as the equivalance classes formed by (mod n) operation

i.e 0, - (n-1) $\{3, 6, 9, \ldots\} = [0]_3$ $n=3$

Z_n^* is the set of numbers that have multiplicative inverses (mod n)

(see the book for more formal definitions of Z_n & Z_n^*)

$\phi(n)$ = the size of Z_n^*, i.e,

$\phi(7) = 6$ [number of integer between 1, .., n-1 that is relatively prime to n.]

Thm 13: $\forall n, m > 0$ with $\gcd(m, n) = 1$
then $\phi(mn) = \phi(m)\,\phi(n)$
$\phi(3 \cdot 7) = 2 \cdot 6 = 12$

Proof:

$\rho : Z_{nm} \to Z_n \times Z_m \quad a \to (b, b')$

First ρ is a function because

$a \equiv a' \pmod{nm}$

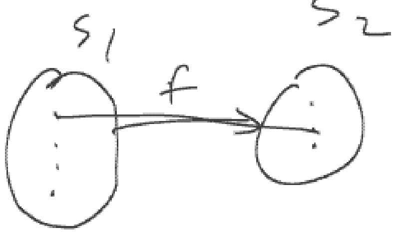
$a \equiv a' \pmod{n}$ & $a \equiv a' \pmod{m}$

ρ is one to one & onto
(Because of Chineese Remainder Thm)

Also $\gcd(a, nm) = 1$ iff
$\gcd(a, n) = 1$ &
$\gcd(a, m) = 1$
(why?)
$z \equiv a_1 \mod n$
$z \equiv a_2 \mod m$

ρ is an injective map
$\mathbb{Z}_{nm}^* \text{ to } \mathbb{Z}_n^* \times \mathbb{Z}_m^*$

$$\Rightarrow |\mathbb{Z}_{nm}^*| = |\mathbb{Z}_n^* \times \mathbb{Z}_m^*|$$



ERROR: undefined
OFFENDING COMMAND:

STACK: