Continuation of Number Theory

extended Euclidean algorithm :

$\forall n, m \in \mathbb{N} \quad \exists\, a, b : \quad am + bn = \gcd(m, n)$

Previous application : If $\gcd(m,n) = 1 \quad \exists\, n^{-1} : \quad n \cdot n^{-1} \equiv 1 \pmod m$

Chinese Remainder Theorem

Suppose we have some $n \in \mathbb{N}$ and know that $n \bmod m_1 = n_1$

$n \bmod m_2 = n_2$

Can we determine n from this information ?

CRT : for any remainders n_1, n_2 (with $\gcd(n_1, n_2) = 1$) $\exists!\, n$ satisfying the equations with $0 \leq n < m_1 m_2$

an example :

$m_1 = 3 \qquad m_2 = 2$

n	$n \bmod m_1$	$n \bmod m_2$
0	0	0
1	1	1
2	2	0
3	0	1
4	1	0
5	2	1
6	0	0

two wheels turning : one every 3 steps , one every two steps .
So the pattern matches again at $n = 6$.

$\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$.
isomorphic

this means $+$ and $*$ work same way on both sides

$$\begin{array}{r} 2 \\ +\ 4 \\ \hline 6 \\ \hline (6 \bmod 6) \end{array} \qquad \begin{array}{r} (2, 0) \\ +\ (1, 0) \\ \hline (0, 0) \end{array}$$

2 mod 3 , 2 mod 2

4 mod 3 , 4 mod 2

3 mod 3 0 mod 2

~~Proof : Find~~

Proof : we are given n_1, n_2 and want to find n : $n \equiv n_1 \pmod{m_1}$, $n \equiv n_2 \pmod{m_2}$

Method : Find solutions for $(1,0)$ and $(0,1)$ first

Lemma : if $\underbrace{m \mid m'}$ then $(n \bmod m') \bmod m = n \bmod m$

$\downarrow$

$m' = k m$ for some k

$r = n \bmod m$ if $\exists q : qm + r = n$

$r' = n \bmod m'$ if $\exists q' : q'm' + r' = n$

$r'' = (n \bmod m') \bmod m$ if $\exists q'' : q''m + r'' = n \bmod m' = r'$

fml

claim is $r'' = r$

$\cancel{n = qm + r \neq q' k m + r'}$

$\cancel{r'' - r}$

$n = r' + q'm'$ $\quad n = r + qm$ $\quad r'' = r' - q''m$

$r' = n - q'm'$ $\quad r = n - qm$

$$r'' - r = [r' - q''m] - [n - qm]$$

$$= r' - n \pmod{m}$$

$r' = n - q'm' = n - q'km$

$r' = n \pmod{m}$

$= 0$

Want to find the equivalent in $\mathbb{Z}_{m_1 m_2}$ of $(1,0)$ in $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$

$b_1 = 1 \pmod{m_1}$

$b_1 = 0 \pmod{m_2} \longrightarrow \quad b_1 = k m_2$ for some k

$$b_1 = k m_2 = 1 \pmod{m_1}$$

Let $k = m_2^{-1} \pmod{m_1}$

$$b_1 = \left(m_2^{-1} \pmod{m_1}\right) m_2$$

$$b_2 = \left(m_1^{-1} \pmod{m_2}\right) m_1$$

example: $m_1 = 3 \quad m_2 = 2$

$\left(m_2^{-1} \pmod 3\right) = 2$ because $2 \cdot 2 = 4 = 1 \pmod 3$

$$(1,0) \rightarrow 4$$
$$(0,1) \longrightarrow 3$$

Always

Claim: having found $b_1 = \left(m_2^{-1} \pmod{m_1}\right) m_2$

$b_2 = \left(m_1^{-1} \pmod{m_2}\right) m_1$

Then we can represent (n_1, n_2) as $n = (n_1 b_1 + n_2 b_2) \bmod m_1 m_2$

example: $n \bmod 3 = 2$, $n \bmod 2 = 1$

then $n = 2 \cdot 2 + 3 \cdot 1 = 5$

and $(5 \bmod 3) = 2$ and $(5 \bmod 2) = 1$

another example:

$m_1 = 7 \quad m_2 = 12 \quad m_1 m_2 = 84$

given: $n \bmod 7 = 4 \quad n \bmod 12 = 3$

What is n? (upto mod 84?)

compute basis elements

$$(1,0) \longrightarrow (\underbrace{12^{-1} \pmod 7}) \cdot 12$$

$$= 3 \cdot 12 = 36$$

$36 = (1 \bmod 7) \qquad 36 = (0 \bmod 12)$

$$(0,1) \longrightarrow (7^{-1} \pmod{12}) \cdot 7$$

$$= 7 \cdot 7 = 49$$

7
14
21
28
35
42
$49 = 4 \cdot 12 + 1$

Solution for n:

$$n = 4 * 36 + 3 * 49$$

$$= 291 \quad \bmod 84$$

$$= 39$$

$39 \bmod 7 = 4$

$39 \bmod 12 = 3$

IF $\gcd(m_1, m_2) = 1$ then $\mathbb{Z}_{m_1 m_2} \approx \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$

iso morphic

i.e. $\exists! \, n \in \mathbb{Z}_m$: $n \bmod m_1 = n_1$
$n \bmod m_2 = n_2$

General / Full version of this thing:

If $m_1, \dots m_k$ are pairwise relatively prime

i.e. $\forall i, j$ if $i \neq j$ then $\gcd(m_i, m_j) = 1$

Then, for any system of equations

$n = n_1 \pmod{m_1}$

$n = n_2 \pmod{m_2}$

$\vdots$

$n = nk \pmod{nk}$

$\exists! \, n \quad 0 \leq n < \prod_{i=1}^{k} m_i$

that satisfies these equations

(x_1, x_2)

Proof : Let $n = \sum_{i=1}^{k} n_i b_i \pmod{\prod m_i}$

where b_i represents $(0, 0, 0, 1, 0\ 0)$ ↑ position i

because $b_i = \left(\prod_{j \neq i} (m_j^{-1} \pmod{i}) \right) \prod_{j \neq i} m_j \begin{bmatrix} = 0 \bmod m_j, & j \neq i \\ = 1 \bmod m_i \end{bmatrix}$

Euler's Theorem :

Start with the definition of totient of n

$$\varphi(n) = |\mathbb{Z}^*_m|$$

$$= |\{x \in \mathbb{Z}_m \mid \gcd(x, m) = 1\}|$$

$$\mathbb{Z}^*_m = \{x \in \mathbb{Z}_m \mid x^{-1} \text{ exists}\}$$

If $m = p$, p is prime

$$\mathbb{Z}^*_p = \{1 \ldots, \ldots p-1\}$$

$$\Rightarrow \varphi(p) = p - 1$$

$m = pq$, $p + q$ both prime

Use CRT

$$x \in \mathbb{Z}_{pq} \longrightarrow (x_1, x_2) \in \mathbb{Z}_p \times \mathbb{Z}_q$$

↑ has inverse if both x_1 and x_2 have inv.

$$(x_1^{-1}, x_2^{-1})$$

no inverse if either x_1 or $x_2 = 0$

$$(1,0)\cdot(x,y) = (x,0)$$

In $\mathbb{Z}_6 = 1 = (\overset{\mathbb{Z}_3}{1}, \overset{\mathbb{Z}_2}{1})$ has inverse $(1,1)$

$1 \cdot 1 = 1 \pmod 6$

$5 = (2,1)$ has inverse $(2,1)$

$5 \cdot 5 = 25 = 1 \pmod 6$

$$\varphi(6) = \varphi(2)\cdot\varphi(3)$$
$$= 2$$

$$\varphi(pq) = (p-1)(q-1)$$

In general, if n factors as

$$\prod_{i=1}^{k} p_i^{e_i}$$

p

$$\varphi(n) = \prod_{i=1}^{k}\left((p_i-1)\,p_i^{e_i-1}\right)$$

Euler's thm: If $\gcd(x,m) = 1$ then $x^{\varphi(m)} = 1 \pmod m$

example: Let $x = 2$

$m = 7$ $\quad 2^{\varphi(m)} = 2^6 = 64 = 9\cdot 7 + 1$

$= 1 \pmod 7$

$m = 15$

$\varphi(15) = \varphi(3)\,\varphi(5)$

$= 2 \cdot 4$

$= 8$

$2^8 \bmod 15 = 256 \bmod 15$

$= 1 \pmod{15}$

~~$m = 3$~~

$3^4 \bmod 5$

$= 81 \bmod 5$

$= 1$

Proof: Given x such that $\gcd(x, m) = 1$

Look at $\mathbb{Z}^*_m$

$x \cdot \mathbb{Z}^*_m = \{ xy \mid y \in \mathbb{Z}^*_m \}$

because $\gcd(x, m) = 1$, x has a inverse.

so $x^{-1} x \mathbb{Z}^*_m = \mathbb{Z}^*_m$

$\rightarrow f(y) \cdot \mathbb{Z}^K \rightarrow x\mathbb{Z}^*_m$

given by $f(y) = xy$ is a bijection

$\Rightarrow |x\mathbb{Z}^*_m| = |\mathbb{Z}^*_m|$

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

[If $y \in \mathbb{Z}^*_m$, y^{-1} exists, but then $(xy)^{-1} = x^{-1}y^{-1}$ also exists

$\mathbb{Z}^*_m$ is finite

$\rightarrow x\mathbb{Z}^*_m = \mathbb{Z}^*_m$

Compute

$$\prod_{y \in \mathbb{Z}^*_m} y = \prod_{xy \in x\mathbb{Z}^*_m} xy = x^{\varphi(m)} \prod_{y \in \mathbb{Z}^*_m} y.$$

Multiply both sides by $\left(\prod y\right)^{-1}$ to get

$$1 = x^{\varphi(m)}$$

RSA encryption

Find two large primes p and q. don't tell anybody what they are!

Pick secret e such that $\gcd(e, \varphi(pq)) = 1$

~~Compute~~ $\varphi(pq) = (p-1)(q-1)$

Compute secret $d = e^{-1} \pmod{(p-1)(q-1)}$

Tell everybody e ~~[illegible]~~

Alice

message $x \longrightarrow x^e \bmod m \longrightarrow$

Bob

$(x^e)^d = x^{k\varphi(m)+1}$ $(\bmod\ m)$

$= 1^k \cdot x = x$

by $\left(\prod x\right)^{-1}$

to get

$1 = x^{\varphi(m)}$