THEORY OF NUMBERS
CONGRUENCES

A reduced set of residues (mod m) is a set of $\phi(m)$ numbers, one from each of the residue classes relatively prime to m.
e.g. $m = 10$ C.S.R.=$0\ \pm 1\ \pm 2\ \pm 3\ \pm 4\ \pm 5$ R.S.R=$\pm 1\ \pm 3$

Theorem Suppose $(k,\ m) = 1$ then if x runs through a C.S.R. or R.S.R. so does kx

Proof (i) kx takes m values and no two are congruent mod m since $kx_1 \equiv kx_2 \Rightarrow x_1 = x_2$ as $(k,\ m) = 1$

(ii) kx takes $\phi(m)$ values, mutually uncongruent mod m, as m (i), and $(kx,\ m) = (x,\ m) = 1$ as $(k,\ m) = 1$.

Theorem (Fermat-Euler) $a^{\phi(m)} = 1$ mod m if $(a,\ m) = 1$

Proof Let $x_1, x_2 \ldots x_{\phi(m)}$ be a R.S.R. mod m. By the previous theorem, $ax_1, ax_2, \ldots ax_{\phi(m)}$ is a R.S.R mod m. Hence these numbers are congruent to $x_1 x_2 \ldots x_{\phi(m)}$ in some order. Therefore

$$ax_1 ax_2 \ldots ax_{\phi(m)} \equiv x_1 x_2 \ldots x_{\phi(m)}\ (m)$$

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

Corollary $a^{p-1} \equiv 1$ mod p if $a \not\equiv 0$ mod p

$a^p \equiv a$ mod p for all a.

Linear congruences $ax \equiv b$ mod m ($a \not\equiv 0$ mod m). N.S.C. for solubility are the N.S.C. for integral solutions $x,\ y$ of $ax - my = b$ i.e. $(a,\ m)|b$.

General solution Suppose $x_0,\ y_0$ is a particular solution of $ax - my = b$ and $x,\ y$ the general solutions therefore

$$a(x_0 - x) - m(y_0 - y) = 0 \tag{1}$$

therefore $m'|x - x_0$ where $m' = \frac{m}{(a,\ m)}$ and $a'|y - y_0$ where $a' = \frac{a}{(a,\ m)}$

therefore

$x = x\_0 + m't$
$y = y_0 + a'l$

Substituting $m(1)$ gives $t = l$, therefore

$x = x_0 + m't$
$y = y_0 + a't$

giving different solutions for $t = 1, 2, \ldots \frac{m}{m'}$, all other solutions belonging to one of these residue classes mod m therefore $\exists (a,\ m)$ solutions.

The Chinese Remainder Theorem If every pair from $(m_1, \ldots, m_r)$ is relatively prime, the simultaneous congruences

$x \equiv a_1 \bmod m_1, \ldots x \equiv a_r \bmod m_r$

have a solution which is unique mod $m_1, \ldots m_r$.

Proof Put

$$M_j = \frac{\prod_{i=1}^{r} m_i}{m_j} \quad j = 1, 2, \ldots, r$$

Choose ξ_j such that $M_j \xi_j \equiv a_j \bmod m_j$

This is possible since $(M_j,\ m_j) = 1$. Note that $M_j \xi_j = 0 \bmod m_i,\ i \neq j$

Take $x = M_1\xi_1 + M_2\xi_2 + \ldots + M_r\xi_r$. Then $x \equiv a_j \bmod m_j\ j = 1, 2, \ldots r$.

Suppose $x_1,\ x_2$ are solutions. Then $x_1 \equiv a_i \bmod m_i\ i = 1, 2, \ldots r,\ x_2 \equiv a_i \bmod m_i\ i = 1, 2, \ldots, r$. Therefore $x_1 - x_2 \equiv 0 \bmod m_i,\ i = 1, 2, \ldots r$ therefore $x_1 - x_2 \equiv 0 \bmod m_1 m_2 \ldots m_r$.

Corollary The congruence $P(x) \equiv 0 \bmod m$ is equivalent to the simultaneous congruences $P(x) \equiv 0 \bmod p_i^{r_i}\ i = 1, 2, \ldots n$.

Theorem Suppose $(a,\ b) = 1$.

Suppose x runs through a $\left\{ \begin{array}{c} C.S.R. \\ R.S.R \end{array} \right\}$ mod a

Suppose y runs through a $\left\{ \begin{array}{c} C.S.R. \\ R.S.R \end{array} \right\}$ mod b

Then $bx + ay$ runs through a $\left\{ \begin{array}{c} C.S.R. \\ R.S.R \end{array} \right\}$ mod ab.

Proof C.S.R

There are ab values of $bx + ay$ and no two are congruent mod ab, for if $bx + ay \equiv bx' + ay' \bmod ab$ then $bx \equiv bx' \bmod a$ and $ay = ay' \bmod b$ since $(ab) = 1$ therefore $x = x' \bmod a$ and $y = y' \bmod b$.

R.S.R

No two values of $bx + ay$ are congruent mod ab as above. All values of $bx + ay$ are relatively prime to ab, for suppose $p|ax + by|$ and $p|ab$.

Then $p|a$ or $p|b$ so suppose $p|a$. $p \not| b$ as $(a,\ b) = 1$ therefore $p|x$. But $(a,\ x) = 1$ as $x \in$ R.S.R. mod a

Conversely every number m relatively prime to ab is congruent to some $bx + ay$ mod ab for if $(ab,\ m) = 1$ choose $x,\ y$ so that

$$\begin{array}{lll} bx \equiv m & \bmod a & \left\{ \begin{array}{l} \text{unique as } (a,\ b) = 1 \text{ and } (a,\ x) = 1 \\ \text{unique as } (a,\ b) = 1 \text{ and } (b,\ y) = 1. \end{array} \right. \\ ay \equiv m & \bmod b & \end{array}$$

Therefore $bx + ay \equiv m$ mod a and mod b and so mod ab as $(a, b) = 1$.

Corollary $\pi(a,\ b) = \phi(a)\phi(b)$ if $(a,\ b) = 1$.

Wilson's Theorem p is prime $\Leftrightarrow (p-1)! \equiv -1$ mod p.

Proof (i) $(p-1)! \equiv -1$ mod $p \Rightarrow (p-1)! + 1 = np$ for some integer n.

Now none of the numbers $2, 3, \ldots p-1$ divides $(p-1)! + 1$, for each of them leaves remainder 1 and so $2, 3, \ldots p-1$ do not divide p. So p is prime.

(ii) $p = 2$ gives $1! \equiv -1$ mod 2, $p = 3$ gives $2! = -1$ mod 3.

Suppose $p > 3$. For every $x \not\equiv 0$ mod $p \exists$ a unique x' mod p such that $xx' \equiv 1$ mod p. If we also have $x \equiv x'$ mod p then $x^2 \equiv 1$ mod p.

i.e. $p|x^2 - 1$ i.e.$p|x - 1$ or $x + 1$ therefore $x \equiv \pm 1$ mod p.

Thus in the product $2, 3, \ldots p-2$ the factors can be associated in pairs, the product of each pair being $\equiv 1$ mod p.

Hence $(p-2)! \equiv 1$ mod p therefore $(p-1)! \equiv p - 1 \equiv -1$ mod p.

The residue classes mod p form a finite field.

Definition Let $(a, m) = 1$. Suppose f is the least positive integer for which $a^f \equiv 1$ mod m. Then we say that a belongs to the exponent f mod m.

Note that $a^s \equiv 1$ mod $m \Leftrightarrow f|s$

(i) $f|s \Rightarrow s = qf$
$a^s = (a^f)^q \equiv 1^q \equiv 1$ mod m.

(ii) $a^s \equiv 1$ mod m
$s = qf + r \ o \leq r < f$
Therefore $(a^f)^q.a^r \equiv 1$ mod m
therefore $a^r \equiv 1$ mod m
therefore $r = 0$ by definition of f and $so f|s$
In particular $f|\phi(m)$ since $a^{\phi(m)} \equiv 1$ mod m.

Theorem Let p be prime and let f be a divisor of $p-1$. Then among a R.S.R. mod p there are exactly $\phi(f)$ elements belonging to the exponent f mod p.

In particular there are $\pi(p-1)$ elements belonging to the exponent $p-1$ mod p: sich an element is known as a primitive root mod p.

Proof Let $\psi(f)$ be the number of elements belonging to the exponent f. We prove

(1) $\psi(f) = 0$ or $\phi(f)$

Suppose $f|p-1$ and suppose $\psi(f) \neq 0$. Then $\exists a$, belonging to exponent f. $1, a, a^2 \dots a^{f-1}$ are uncongruent mod p, but all satisfy $x^f \equiv 1 \bmod p$. So they are all solutions of $x^f \equiv 1$

Thus the numbers belonging to exponent f are to be found among these.

We show that a'' belongs to $\exp f \Leftrightarrow (v,\ f = 1$. Suppose a'' belongs to $\exp f'(:\ f'|f)$

(i) $(v,\ f) = 1$ Suppose $(a'')^f \equiv 1 \bmod p$ then $a''f \equiv 1 \bmod p$ but a belongs to $\exp f$ and so $f|vf'$ therefore $\|f'$ so $f = f'$.

(ii) $(v, f) = d > 1$

$(a^v)^{\frac{f}{d}} \equiv (a^f)^{\frac{v}{d}} \equiv 1 \bmod p$ since a belongs to $\exp f$.

Thus a'' doesn't belong to $\exp f$ since $\frac{f}{d} < f$. Hence $\psi(f) = \phi(f)$.

We now prove

(2) $\sum_{f|p-1} \psi(f) = p-1$

Every residue $\not\equiv 0 \bmod p$ belongs to exactly one exponent f and $a^f \equiv 1 \bmod p \Leftrightarrow f|p-1$ for $a^{p-1} \equiv 1$ by Fermats theorem.

But $\sum_{f|p-1} \phi(f) = p-1$

So $\sum_{f|p-1} [\phi(f) - \psi(f)] = 0,\ [\phi(f) - \psi(f)] \geq 0$ by (1) therefore $\phi(f) = \psi(f)$.

Indices Suppose g is a primitive root mod p, $p > 2$.

Then $g^0, g^1, g^2, \dots, g^{p-2}$ constitute an R.S.R. mod p.

For each a satisfying $(a,\ p) = 1 \exists$ a unique integer r such that $g^r \equiv a$ mod p $0 \leq r \leq p-2$

We write $r = md_g a$.

Then $a \equiv b \bmod p \Leftrightarrow md_g a = md_g b$

$$\left.\begin{array}{c} md_g a^n = n md_g a \\ md_g ab = md_g a + md_g b \\ md_g a = md_g g; md_{g'} a \end{array}\right\} \bmod p-1$$

$md1 = 0$

$md - 1 = \frac{p-1}{2}$, for $g^{p-1} \equiv 0$ so $\left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) \equiv 0$ but $g^{\frac{p-1}{2}} \not\equiv 1$ as g is a primitive root so $g^{\frac{p-1}{2}} \equiv -1$

Example

$p = 13 \quad g = 2$

N	Index
1	0
2	1
4	2
8	3
3	4
6	5
12	6
11	7
9	8
5	9
10	10
7	11

Example $\sum_{n=1}^{p-1} n^s \equiv \begin{cases} 0 & \bmod p \text{ if } s \not\equiv 0 \bmod p-1 \\ -1 & \bmod p \text{ if } s \equiv 0 \bmod p-1 \end{cases}$