

18.781

24 Feb 2003

Residue System

$$m \in \mathbb{Z}$$

complete residue system: set $\{r_1, \dots, r_m\}$ s.t. any n is \equiv to exactly one r_i

Reduced residue system: set $\{r_1, \dots, r_\phi\}$ s.t. $(r_i, m) = 1$ and for any $(n, m) = 1$,

there exists exactly one r_i with $r_i \equiv n \pmod{m}$

$\phi(m) = \#$ of elts in any reduced residue syst.

$= \#$ of integers $0 < n < m$ with $(n, m) = 1$.

Thrm: If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Lemma: If $(a, m) = 1$ and $\{r_1, \dots, r_\phi\}$ is a reduced residue syst, then

$\{ar_1, \dots, ar_\phi\}$ is also a reduced residue system.

Proof: since $\#$ of elts in $\{ar_i\} = \#$ elts. in $\{r_i\}$, it is enough to show

$(ar_i, m) = 1$ and $ar_i \not\equiv ar_j \pmod{m}$, $\forall i, j$

$$(ar_i, m) = 1$$

if $(a, m) = 1$, then $(an, m) = (n, m)$, $(r_i, m) = 1$. $\therefore (ar_i, m) = 1$

$$ar_i \not\equiv ar_j \pmod{m}$$

$m \nmid a(r_i - r_j)$, since $(m, a) = 1$ and by distinctness of reduced res. system elts, $m \nmid (r_i - r_j)$.

Proof of Thrm:

$$\{r_1, \dots, r_{\phi(m)}\} \quad \{ar_1, \dots, ar_{\phi(m)}\}$$

For each r_i , $\exists! j$ s.t. $r_i \equiv ar_j \pmod{m}$

$$r_1 \dots r_{\phi(m)} \equiv (ar_1) \dots (ar_{\phi(m)}) \pmod{m} \Rightarrow$$

$$r_1 \dots r_{\phi(m)} \equiv a^{\phi(m)} (r_1 \dots r_{\phi(m)}) \pmod{m}$$

(can cancel $r_1 \dots r_{\phi(m)}$ since $(r_1 \dots r_{\phi(m)}, m) = 1$.)

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

Corollary: If p prime, then for any a s.t. $(a, p) = 1$, $a^p \equiv a \pmod{p}$.

Proof: $a^p \equiv a \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$. (since $(a, p) = 1$.)

$$\phi(p) = \# \text{ integers in } [1, p] \text{ prime to } p = p-1.$$

Ex: If a and b prime to 13, then $13 \mid (a^{12} - b^{12})$.

$$\text{Look at } a^{12} - b^{12} \equiv 1 - 1 \equiv 0 \pmod{13}$$

Question: Given m and a , does there exist b s.t. $ab \equiv 1 \pmod{m}$?

Thrm: If $(a, m) = 1$, \exists such b , in which case b is unique up to adding multiples of m .

Proof: $ab \equiv 1 \pmod{m}$ means $\exists y$ s.t. $ab + my = 1$.

If $(a, m) = 1$, $\exists x + y$ s.t. $ax + my = 1$.

If $ab + my = 1$, then $g = (a, m)$ and $g \mid ab + my \Rightarrow g \mid 1 \Rightarrow g = 1$.

Cor. If p is prime and $x^2 \equiv 1 \pmod{p}$, then $x \equiv \pm 1 \pmod{p}$.

Proof:

If $p=2$, it's okay.

otherwise, $(x+1)(x-1) \equiv 0 \pmod{p} \Rightarrow p \mid (x+1)$ or $(x-1)$.

Cor. (Wilson's Thrm).

If p is prime, $(p-1)! \equiv -1 \pmod{p}$.

Proof: Let $\{r_1, \dots, r_{p-1}\}$ be a reduced residue syst. e.g. $\{1, \dots, p-1\}$.

Look at $r_1 \dots r_{p-1}$.

ex: $p=5$, $1, 2, 3, 4$, $2 \cdot 3 = 6 \equiv 1 \pmod{5}$

$1 \cdot 2 \cdot 3 \cdot 4 \equiv 4 \pmod{5} \equiv -1 \pmod{5}$

Need to know when $r_i^2 \equiv 1 \pmod{p}$, since otherwise $r_i^{-1} \in \{r_j\}_{j \neq i}$.

This is when $r_i \equiv 1$ or $p-1 \pmod{p}$.

$\therefore 1 \cdot 2 \dots p-2 \cdot p-1 \equiv 1 \cdot p-1 \equiv p-1 \equiv -1 \pmod{p}$.

Question: Given $n \in \mathbb{Z}$, when can you write n as a sum of 2 squares, i.e. $n = a^2 + b^2$?

Thrm: $n = 2^a \prod_{p \equiv 1 \pmod{4}} p^{\alpha_p} \prod_{p \equiv 3 \pmod{4}} p^{\beta_p}$. Then $n = a^2 + b^2$ iff all β_p are even.

ex: $n = 102 = 2 \cdot 51 = 2 \cdot 3 \cdot 17$. 3 is only prime $\equiv 3 \pmod{4}$. Since exp. odd, $102 \neq a^2 + b^2$.

ex: $n = 549 = 225 + 324$

$549 = 3 \cdot 183 = 9 \cdot 61 = 3^2 \cdot 61$. $61 \equiv 1 \pmod{4}$, $3 \equiv 3 \pmod{4}$, and exp. even.