Math 312, lecture 9, 29/5/2018

Final Exam: Tuesday, June 26th, 15:30 at LSK 201.

PS1: Available tomorrow at filing cabinet next to MATH 225.

Last time: CRT

(1) $M = m_1 m_2$ (eg. $35 = 5 \cdot 7$)

- Every class mod M determines a class mod m_1
- Every class mod m_1 " m_2 classes mod M:

$a \rightsquigarrow a, a+m_1, a+2m_1, a+3m_1, \ldots, a+(m_2-1)m_1$

(2) A class a_1 mod m_1 + a class a_2 mod m_2 determine a class a mod M

$a \equiv 1 (5)$ + $a \equiv -1 (7)$ $\Rightarrow$ $a \equiv 6 (35)$

$a \equiv 2 (5)$ and $a \equiv -1 (7)$

Brute force: class is one of $-1, 6, 13, 20, 27$ (mod 35)

of those, $27 \equiv 2 (5)$ so $a \equiv 27 (35)$

Example 6: Let p, q be distinct odd primes

Then have 4 solutions to $x^2 \equiv 1 \ (pq)$

Computational approach:

Say $M = m_1 \cdots m_r$, $(m_i, m_j) = 1$ if $i \neq j$.

(e.g. $M = 2^5\, 3^7 \cdot 7^{11} \cdot 13 \cdots$)

Observe: if $i \neq j$ m_j is invertible mod m_i, so $\prod_{j \neq i} m_j = N_i$ is also invertible.

$\boxed{N_i = \frac{M}{m_i}}$ (promise: $(N_i, m_i) = 1$)

Aside: x_i is $\overline{N_i}$, the modular inverse of N_i mod m_i

Bezout: find x_i, y_i s.t. $\boxed{N_i x_i + m_i y_i = 1}$

set $\boxed{b_i = N_i x_i}$ $\left(\begin{array}{l} b_i \equiv 1 \ (m_i) \\ b_i \equiv 0 \ (m_j) \text{ if } j \neq i \end{array}\right)$

Given a_i mod m_i set

$$\boxed{a = \sum_{i=1}^{r} a_i b_i}$$

Example: Find a mod 105 s.t. $\begin{cases} x \equiv 1 \ (3) \\ x \equiv 2 \ (5) \\ x \equiv 3 \ (7) \end{cases}$

2-2

Solution: Need b_1 s.t. $\begin{array}{l} b_1 \equiv 1 \ (3) \\ b_1 \equiv 0 \ (35) \end{array}$: $35 \equiv 2 \ (3)$ so $2 \cdot 35 \equiv 1 \ (3)$

take $b_1 = 70$ ($b_1 = -35$ also works)

Need b_2 s.t. $\begin{array}{l} b_2 \equiv 1 \ (5) \\ b_2 \equiv 0 \ (21) \end{array}$ eg. $b_2 = 21$

Need b_3 s.t. $b_3 \equiv 1 \ (7)$ eg. $b_3 = 15$.

<u>Questions:</u> Find

$1!$ mod 2		$1! = 1 \equiv 1\ (2)$
$2!$ mod 3		$2! = 2 \equiv 2\ (3)$
$4!$ mod 5		$4! = 24 \equiv 4\ (5)$
$6!$ mod 7		$6! = 720 \equiv 20 \equiv 6\ (7)$
$10!$ mod 11		

$3\cdot 4 \equiv 1 (11)$ $\quad$ $5\cdot 9 = 45 \equiv 1\ (11)$

$$1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10 \equiv 10 \quad (11)$$

$2\cdot 6 \equiv 1 (11)$ $\quad$ $7\cdot 8 = 56 = 55+1 \equiv 1 (11)$

<u>Thm:</u> (Wilson) Let p be prime. Then $(p-1)! \equiv p-1 \equiv -1 \pmod p$

<u>Pf:</u> This is $\prod_{a \in U(p)} a$ pair up every residue class with its inverse class. As long as $a^2 \not\equiv 1$, $a \neq \bar{a}$, so both $a, \bar{a}$ occur

p prime so all classes $1 \leq a \leq p-1$ are invertible

and ~~cancel~~ cancel each other out.

Left with: $\prod_{a \in U(p)} \equiv \prod_{a : a^2 = 1} a \equiv 1\cdot(-1) \equiv -1 \equiv p-1\ (p)$

<u>Example:</u> What is $\frac{10!}{8}$ mod 11?

<u>Ideas:</u>
- Modular inverses
- List all invertible residues

Multiplicative order:

Powers of 2 mod 7:

$$2^0 \equiv 1 \ (7)$$
$$2^1 \equiv 2 \ (7)$$
$$2^2 \equiv 4 \ (7)$$
$$2^3 \equiv 2 \cdot 4 \equiv 8 \equiv 1 \ (7)$$
$$2^4 \equiv 2 \cdot 2^3 \equiv 2 \cdot 1 \equiv 2 \ (7)$$
$$2^5 \equiv 4 \ (7)$$
$$2^6 \equiv 1 \ (7)$$
$$\vdots$$

mod 11: $2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 5$,

$2^5 \equiv 10 \equiv -1$, $2^6 \equiv -2$, $2^7 \equiv -4$, $2^8 \equiv -8$, $2^9 \equiv -5$

$2^{10} \equiv -10 \equiv 1$

5 mod 11: $5^0 \equiv 1$, $5^2 \equiv 3$, $5^3 \equiv 4$, $5^4 \equiv -2$, $5^5 \equiv 1$

Def: Let $(a,m)=1$. The multiplicative order of a mod m is the least positive k s.t. $a^k \equiv 1 \ (m)$ (write: $k = \mathrm{ord}_m(a)$)

Saw: $\mathrm{ord}_7(2) = 3$, $\mathrm{ord}_{11}(2) = 10$, $\mathrm{ord}_{11}(5) = 5$

Prop: (1) $\exists k \geq 1$ s.t. $a^k \equiv 1 \ (m)$

(2) $a^r \equiv a^s \ (m)$ iff $r \equiv s \ (\mathrm{ord}_m(a))$

$2^r \equiv 2^s \bmod (7)$ iff $r \equiv s \ (3)$

Pf: (1) Consider the numbers $\{a^0, a^1, a^2, .., a^m\}$

these are $m+1$ elements of $U(m)$, a set of size $\le m$

so (by pigeonhole principle) have $r \ne s$ s.t. $a^r \equiv a^s \ (m)$

~~then~~ wlog $r > s$, then $a^{r-s} \equiv a^{s-s} \equiv 1 \ (m)$ and $r-s>0$.

(a^{-1} means $\bar{a}$, a^{-n} means $(\bar{a})^n$ if $n \ge 0$)

(2) wlog $r \ge s$, $r = s+t$. If $\mathrm{ord}_m(a) \mid t$

then $a^r \equiv a^{s+t} \equiv a^s \cdot a^t = a^s \cdot \left(a^{\mathrm{ord}_m(a)}\right)^{\frac{t}{\mathrm{ord}_m(a)}} \equiv a^s \cdot 1^{\frac{t}{\mathrm{ord}_m(a)}} \equiv a^s \ (m)$

Conversely, if $a^r \equiv a^s$ then $a^{r-s} \equiv 1 \ (m)$

write $r-s = q \cdot \mathrm{ord}_m(a) + u$, $0 \le u < \mathrm{ord}_m(a)$

then $1 \equiv a^{r-s} \equiv a^{q \cdot \mathrm{ord}_m(a) + u} \equiv \left(a^{\mathrm{ord}_m(a)}\right)^q \cdot a^u \equiv a^u \ (m)$

$a^{\mathrm{ord}_m(a)} \equiv 1$

But $u < \mathrm{ord}_m(a)$, and $\mathrm{ord}_m(a)$ was smallest positive s.t. $a^k \equiv 1$.

so u is not positive, i.e. $u = 0$

and $r - s = q \cdot \mathrm{ord}_m(a) \equiv 0 \ (\mathrm{ord}_m(a))$

Warning: When computing a^r mod m, can reduce a mod m

can reduce r mod $\mathrm{ord}_m(a)$ (not mod m)

In $2^{1{,}000{,}000} \equiv 2^1 \ (7)$ reduce $1{,}000{,}000$ mod 3 not mod 7.