Lecture 6

$ax \equiv c \bmod m \quad a^{-1}(ax) \equiv a^{-1}c \bmod m \quad$ so $x \equiv a^{-1}c \bmod m$

special case: $\gcd(a,m)=1$

$\boxed{ax \equiv 1 \bmod m, \gcd(a,m)=1}$

$x \equiv a^{-1} \bmod m$

$\cancel{\frac{1}{a}}$

one of $0, 1, \cdots, m-1$

$ax \equiv c \bmod m$. $\gcd(a,m)=g$, $g \mid c$

$x = x_0 + \frac{m}{g}k$, $k=0,\cdots,g-1$

one solution

$\gcd\left(\frac{a}{g}, \frac{m}{g}\right)=1$, $\frac{a}{g}x \equiv \frac{c}{g} \bmod \frac{m}{g}$, $x_0 = \left(\frac{a}{g}\right)^{-1}\left(\frac{c}{g}\right) \bmod \frac{m}{g}$

e.g. $893x \equiv 266 \pmod{2432}$

$\gcd(893, 2432)=19$, $19 \mid 266$

$x = x_0 + \frac{2432}{19}k$, $k=0, 1, \cdots, 18$

divide by 19 : $47x \equiv 14 \bmod 128$

$\gcd(47,128)=1$

$x_0 = 47^{-1} \cdot 14$

$47x \equiv 1 \bmod 128$

$47\underset{-49}{x} - 128\underset{18}{y} = 1$

$128 = 47 \times 2 + 34$

$47 = 34 \times 1 + 13$

$34 = 13 \times 2 + 8$

$13 = 8 \times 1 + 5$

$8 = 5 \times 1 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

$2 = 1 \times 2$

$47^{-1} \equiv -49 \bmod 128$

$\equiv 79 \bmod 128$

$x = 79 \times 14 + 128k \bmod 2432$, $k=0, \cdots, 18$

$x^d + a_1x^{d-1} + \cdots + a_d \equiv 0 \bmod p$ has at most d distinct sols mod p

① Check solvability $x^2 \equiv a \bmod p$

② If a soln exists, find it (all solns)

Chapter 9. Fermat's Little Thm

p prime $a \not\equiv 0 \bmod p$ [This means $p \nmid a$]

Then $a^{p-1} \equiv 1 \bmod p$

$a^6 \bmod 7$

$2^6 \equiv 64 \equiv 1 \bmod 7$

$3^6 \equiv 729 \equiv 1 \bmod 9$

$6^{22} \equiv 1 \bmod 23$

$6^{22} - 1 = 23 \times 5722682775750745$

Before proving, applications:

① Compute $2^{35} \bmod 7$

Use the fact $2^6 \equiv 1 \bmod 7$

$$2^{35} = 2^{6\times5+5} = (2^6)^5 \cdot 2^5 \equiv 1 \cdot 2^5 \equiv 32 \bmod 7 \equiv 4 \bmod 7$$

② We want to solve $x^{103} \equiv 4 \bmod 11$

Assume $x \not\equiv 0$, $x^{10} \equiv 1 \bmod 11$

$$x^{103} \equiv x^{100} \cdot x^3 \equiv x^3 \bmod 11$$

need to solve

$$x^3 \equiv 4 \bmod 11$$

$x \bmod 11$	-5	-4	-3	-2	-1	0	1	2	3	4	5
$x^3 \bmod 11$	-4	2	6	3	-1	0	1	8	5	-2	4

so $x \equiv 5 \bmod 11$ is the only solution.

$n! = n \times (n-1) \times \cdots \times 1$

Trick: We prove that $a, 2a, \cdots, (p-1)a \bmod p$ are the same as $1, 2, \cdots, p-1 \bmod p$

They might shuffle around, even though they might have different order.

e.g. $p=7, a=2$

1 2 3 4 5 6

2 4 6 8 10 12

congruent: $\underline{2\,4\,6\,1\,3\,5}$ (shuffled)

Then $a, 2a, \cdots, (p-1)a \equiv 1, 2, \cdots, p-1 \bmod p$

$a^{p-1}(p-1)! \equiv (p-1)! \bmod p$, $p \nmid (p-1)!$

so $a^{p-1} \equiv 1 \bmod p$

$a, 2a, \cdots, (p-1)a$ not divisible by p.

Claim: If $ja \equiv ka \bmod p$, then $j = k$, $1 \le j \le k \le p-1$

Suppose: $ja \equiv ka \bmod p$, $p \mid (k-j)a$

since $p \nmid a$, then $p \nmid (k-j)$

since $1 \le j \le k \le p-1 \Rightarrow 0 \le k-j < p-1 \Rightarrow k-j = 0$ is the only possibility

Since there are only $p-1$ distinct nonzero #s mod p, we have our result.