Math 312, lecture 11, 31/5/2018

Today: (1) Euler's thm, pseudoprimes
(2) Review

Last time: $\mathrm{ord}_m(a)$ = period in sequence $a^0, a^1, a^2, \ldots \bmod m$
($(a,m)=1$)

Fermat: $a^{p-1} \equiv 1 \ (p)$ if $p \nmid a \Rightarrow \mathrm{ord}_p(a) \mid p-1$.

(later: if $d \mid p-1$ there is a mod p with $\mathrm{ord}_p(a) = d$)

Example: p Sophie Germain prime ($2p+1=q$ is also prime)
Then if $a \not\equiv -1, 0, +1 \bmod q$, $\mathrm{ord}_q(a) \in \{p, 2p\}$.

For practical application need primes (also want to know, e.g. if $2^{2^n}+1$, or 2^p-1 is prime)

Problem: Given n, test whether n is prime

Method of trial division (by $d \le \sqrt{n}$) takes time $\sim \sqrt{n}$.

Better idea: use Fermat's thm:

take a ($a=2$, or a random between $2, n-1$)
Compute $a^{n-1} \bmod n$. If we get $\neq 1$, n may be prime
If not, n is definitely composite

(Say a is a "witness" to n being composite)
(Can compute a^{n-1} efficiently using "repeated squaring" algorithm)

Def: Say n is a <u>pseudoprime to base b</u> if $b^{n-1} \equiv 1 \ (n)$

(eg. pseudoprime to base 2: $n \mid 2^{n-1} - 1$)

Ex: If $a^{n-1} \equiv 1 \ (n)$, $b^{n-1} \equiv 1 \ (n)$ then $\begin{cases} (ab)^{n-1} \equiv 1 \ (n) \\ (\bar{a})^{n-1} \equiv 1 \ (n) \end{cases}$

Cor: If witnesses exist, at <u>least half</u> the residues are witnesses

<u>But</u>: Exist n composite <u>without</u> witnesses (this way)

<u>Goal</u>: Study this.

Def: The Euler (totient) function $\phi(m)$ is given by:

$$\phi(m) = \#\mathcal{U}(m) = \#\{a \mid 1 \le a < m, \ (a,m) = 1\}$$

Eg. $\phi(p) = p - 1$ if p primes

$\phi(8) = \#\{1, 3, 5, 7\} = 4$

$\phi(27) = 27 - \frac{1}{3} \cdot 27 = 18$

↖ $\frac{1}{3}$rd of residues mod 27 are divisible by 3, others are prime to 27.

Thm: (Euler) $a^{\phi(m)} \equiv 1 \ (m)$ if $(a,m) = 1$ $\quad y = ax, \ x = \bar{a}y$

Pf: Let $A \equiv \prod_{(x,m)=1} x \ (m)$. Then $a^{\phi(m)} \cdot A \equiv \prod_{(x,m)=1} (ax) \equiv \prod_{(y,m)=1} y \equiv A \ (m)$

multiply by $\bar{A}$ to get $a^{\phi(m)} \equiv 1 \ (m)$

Consider $n = 561 = 3 \cdot 187 = 3 \cdot 11 \cdot 17$

$5(561) = 12 \equiv 3 (9)$ ↑

$1 - 8 + 7 = 0 \equiv 0 \ (11)$ ↖

$5 \nmid 187$ $(187 \equiv 7 \ (10)$

$7 \nmid 187$ $(187 \equiv 180 \ (7))$

Claim: If $(a, 561)$ then $a^{560} \equiv 1 \ (561)$

Pf: CRT says: $a^{560} \equiv 1 \ (561)$ iff $\begin{cases} a^{560} \equiv 1 \ (3) \\ a^{560} \equiv 1 \ (11) \\ a^{560} \equiv 1 \ (17) \end{cases}$

Fermat's: If $3 \nmid a$ then $a^2 \equiv 1 \ (3)$

so $a^{560} = (a^2)^{280} \equiv 1^{280} \equiv 1 \ (3)$

$(a, 561) = 1$ i.e. $3 \nmid a, 17 \nmid a, 11 \nmid a$

Similarly, since $11 \nmid a$, $a^{10} \equiv 1 \ (11)$ so $a^{560} \equiv (a^{10})^{56} \equiv 1 \ (11)$

$17 \nmid a$, $a^{16} \equiv 1 \ (17)$ so $a^{560} = (a^{16})^{35} \equiv 1 \ (17)$ ✓

Def: Call n a Carmichael number if $(a, n) = 1 \Rightarrow a^{n-1} \equiv 1 \ (n)$ but n is composite.

Next week: $\phi(561) = \phi(3) \cdot \phi(11) \phi(17) = (3-1)(11-1)(17-1) =$

$= 2 \cdot 10 \cdot 16 = 320$

so Euler: If $(a, 561)$, $a^{320} \equiv 1 \ (561)$.

$\Rightarrow a^d \equiv 1 \ (561)$ where $d = (320, 560)$.

Q: Suppose $a^k \equiv 1 \ (n)$ (also) then $(a, n) = 1$:

a, a^k divisible by same primes ↓

As If $a^k \equiv 1 \ (n)$ then $(a^k, n) = (1, n) = 1$ so $(a, n) = 1$.

Aside

Miller identified a stronger notion of witness:

write $n-1 = 2^k \cdot m$, m odd.

Then Fermat: if n is prime, $(a,n)=1$ then $a^{2^k \cdot m} \equiv 1 \ (n)$

write this as $(((a^m)^2)^2)^{2\cdots} \equiv 1$

(k squarings)

If n is prime, either $a^m \equiv 1 \ (n)$ or before $(\ )^2 \equiv 1 \ (n)$ we had $(\ ) \equiv -1 \ (n)$

Call a a "strong witness" if $a^{n-1} \not\equiv 1 \ (n)$ or have $a^{2^\ell m} \not\equiv -1 \ (n)$ while $a^{2^{\ell+1} m} \equiv 1 \ (n)$

Miller: If n is composite it has this kind of witness $a \le 2\log^2 n$ + On Extended Riemann Hypothesis, $\exists$ witness

Rabin: In any case, at least $\frac{1}{2}$ the residues are witnesses so random checking works

Midterm Review

Questions : (1) Calculation
(2) Definitions / Statements of thms
(3) Problems / Proofs

Problems Solve $\begin{cases} x+2y+z \equiv 3 \pmod 7 \\ 4x-y \equiv 1 \pmod 7 \end{cases}$

In one direction, suppose x,y,z is a solution.
Multiplying 2nd equation by 2, get:

$2 \cdot 4 = 8 \equiv 1 \pmod 7$

$$\begin{cases} x+2y+z \equiv 3 \pmod 7 \\ x-2y \equiv 2 \pmod 7 \end{cases}$$

adding & subtracting the equations, we get

$$\begin{cases} 2x+z \equiv 5 \pmod 7 \\ 4y+z \equiv 1 \pmod 7 \end{cases}$$

mult 1st eqn by 4, 2nd by 2 get:

$$\begin{cases} x+4z \equiv 20 \equiv -1 \pmod 7 \\ y+2z \equiv 2 \pmod 7 \end{cases} \quad \text{i.e.} \quad \begin{cases} x \equiv -1-4z \equiv 6+3z \\ y \equiv 2-2z \equiv 2+5z \end{cases} \pmod 7$$

Solutions $\left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 2 \\ 0 \end{pmatrix} + z \cdot \begin{pmatrix} 3 \\ 5 \\ 1 \end{pmatrix} : z \bmod 7 \right\}$

Need to verify, indeed if

$x \equiv 6+3z$
$y \equiv 2+5z$ then $x+2y+z \equiv (6+3z)+(4+10z)+z$
$\equiv 10+14z \equiv 3 \ (7)$ ✓

and $4x-y \equiv 24+12z-2-5z$
$\equiv 22+7z \equiv 1 \ (7)$ ✓

Continuations solve mod 2.

system is: $\begin{cases} x+z \equiv 1 \ (2) \\ +y \equiv 1 \ (2) \end{cases}$ solution is: $\left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \equiv \begin{pmatrix} 1+z \\ 1 \\ z \end{pmatrix} \text{ mod } 4 \right\}$

$\Rightarrow \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + z \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} (2) \right\}$

Mod 14:

Given ~~z~~ mod 14 have $\begin{cases} x \equiv 1+z \ (2) \\ x \equiv 6+3z \ (7) \end{cases}$

note: $\begin{cases} 7 \equiv 1 \ (2) \\ 7 \equiv 0 \ (7) \end{cases}$, $\begin{cases} 8 \equiv 0 \ (2) \\ 8 \equiv 1 \ (7) \end{cases}$ so $x \equiv 7(1+z) + 8 \cdot (6+3z)$

$\equiv 7+48+\cancel{24}^{31}z$

$\equiv -1+\cancel{3}^{3}z \ (14)$

need $\begin{cases} y \equiv 1 \ (2) \\ y \equiv 2+5z \ (7) \end{cases}$ so $y \equiv 7+16+40z$

$\equiv 9+12z \ (14)$

Solutions: $\left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \equiv \begin{pmatrix} -1 \\ 9 \\ 0 \end{pmatrix} + \begin{pmatrix} 3 \\ 12 \\ 1 \end{pmatrix} z \ (14) \right\}$

z arbitrary

Problem: Show by induction that

$$4^n \equiv 1+3n \quad (9)$$

Solution: When $n=0$, $4^n = 1 \equiv 1+3\cdot n$ and the claim holds. Suppose the claim holds for some n. Then

$$4^{n+1} = 4\cdot 4^n \underset{\text{claim for } n}{\equiv} 4(1+3n) \equiv 4+12n$$

$$\equiv 4+3n \equiv 1+3+3n \equiv 1+3(n+1) \quad (9)$$

$$12 \equiv 3 \ (9)$$

and the claim holds for $n+1$.

Prob

Problem: For which c, $0 \le c < 30$, does

$12x \equiv c \pmod{30}$ have solutions?

if so, how many?

Solution. If x is a solution, since $6 \mid 12$ and $6 \mid 30$,

$c \equiv 12x \equiv 0 \pmod 6$, ie $6 \mid c$.

So if $6 \nmid c$ have no solutions.

If, instead, $6 \mid c$, the congruence is equivalent to $2x \equiv \frac{c}{6} \pmod 5$

which is equivalent to $3 \cdot (2x) \equiv 3 \cdot \frac{c}{6} \pmod 5$ ($2 \cdot 3 \equiv 1 \pmod 5$ both are invertible)

ie to $x \equiv \frac{c}{2} \pmod 5$

The class of $\frac{c}{2} \bmod 5$ splits into $6 = \frac{30}{5}$ classes mod 30 so have 6 solutions if $6 \mid c$.

(they are $\frac{c}{2}, \frac{c}{2}+5, \frac{c}{2}+10, \frac{c}{2}+15, \frac{c}{2}+20, \frac{c}{2}+25$ mod 30)

Question: Why are congruences

$12x \equiv c \ (30)$

$2x \equiv \frac{c}{6} \ (5)$

equivalent (if $\frac{c}{6} \in \mathbb{Z}$)?

Because: $12x \equiv c \ (30) \iff 30 \mid 12x - c$

$\iff 12x - c = 30k$ for some $k \in \mathbb{Z}$

$\iff 2x - \frac{c}{6} = 5k$ for some $k \in \mathbb{Z}$

$\iff 2x \equiv \frac{c}{6} \ (5)$

Problem: Solve $\begin{cases} x^2 \equiv 3 \ (6) \\ x^3 \equiv 3 \ (5) \end{cases}$

By CRT, $x^2 \equiv 3 \ (6) \iff \begin{cases} x^2 \equiv 3 \ (2) \\ x^2 \equiv 3 \ (3) \end{cases}$ i.e. $\begin{cases} x^2 \equiv 1 \ (2) \\ x^2 \equiv 0 \ (3) \end{cases}$

2 is prime $\rightarrow \iff \begin{cases} x \equiv 1 \ (2) \\ x \equiv 0 \ (3) \end{cases}$ i.e. $\begin{cases} x \equiv 3 \ (2) \\ x \equiv 3 \ (3) \end{cases} \iff x \equiv 3 \ (6)$

3 is prime $\rightarrow$

what about $x^3 \equiv 3 \ (5)$? since $x^3 \equiv 3 \ (5)$, $5 \nmid x^3$ so $5 \nmid x$

so (Fermat) $x^4 \equiv 1 \ (5)$. By $x^3 \equiv 3 \ (5) \iff x \cdot x^3 \equiv 3x \ (5)$

↑ mult by x

i.e. $3x \equiv 1 \ (5)$ so $x \equiv 2 \ (5)$ (mult by 2)

(or: $0^2 \equiv 0\ (6)$ $0^3 \equiv 0\ (5)$

$1^2 \equiv 1\ (6)$ $1^3 \equiv 1\ (5)$

$2^2 \equiv 4\ (6)$ $2^3 \equiv 3\ (5)$

$3^2 \equiv 3\ (6)$ $3^3 \equiv 2\ (5)$

$4^2 \equiv 4\ (6)$ $4^3 \equiv 4\ (5)$

$5^2 \equiv 1\ (6)$

In any case, the system is equivalent to

$$\begin{cases} X \equiv 3\ (6) \\ X \equiv 2\ (5) \end{cases}$$

By the CRT this

the class of 3 mod 6 contains 3, 9, 15, 21, 27,

so $27 \equiv 3\ (6)$ and $27 \equiv 2\ (5)$.

By CRT we conclude that $X \equiv 27\ (30)$

i.e. $\begin{cases} X^2 \equiv 3\ (6) \\ X^3 \equiv 3\ (5) \end{cases}$ iff $X \equiv 27\ (30)$