Math 312, lecture 17, 12/6/2018

Last week

(1) Arithmetic functions:

- multiplicative function $f(60) = f(4)\cdot f(5)\cdot f(3)$
- Dirichlet convolution $(f*g)(n) \overset{\text{def}}{=} \sum_{d|n} f(d)\,g\left(\frac{n}{d}\right) = \sum_{de=n} f(d)\,g(e)$

$\tau(n) = \sum_{d|n} 1$, $\sigma(n) = \sum_{d|n} d$, ..

$\phi * I = N \leftarrow \boxed{\sum_{d|n} \phi(d) = n}$

- Möbius inversion: $\delta * f = f$, $\mu * I = \delta$ $\quad \delta(n) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$

(2) Cryptography: affine character ciphers ($P \to aP+b \bmod 26$)

→ RSA (block cipher)

computations in multiplicative group mod pq.

$\left(\sum_{d|n} \phi(d) = \sum_{e|n} \phi\left(\frac{n}{e}\right)\right.$ if $d|n$ then $n = d\cdot\frac{n}{d}$

$e = \frac{n}{d}$ $= \sum_{d|n} \#\{a \bmod n \mid \gcd(a,n) = d\} = \#\{a \bmod n\} = n$

residues mod 12 grouped by $\gcd(\cdot,12)$

$n=12$			
$\{1,5,7,11\}$	$\gcd(a,12)=1$	$\{1,5,7,11\} \bmod 12$	
$\{2,10\}$	$\gcd(a,12)=2$	$\to \{1,5\} \bmod \frac{12}{2}=6$	
$\{3,9\}$	$\gcd(a,12)=3$	$\{\frac{3}{3},\frac{9}{3}\}=\{1,3\} \bmod \frac{12}{3}=4$	
$\{4,8\}$	$\gcd(a,12)=4$	$\{\frac{4}{4},\frac{8}{4}\}=\{1,2\} \bmod \frac{12}{4}=3$	
$\{6\}$	$\gcd(a,12)=6$	$\{1\} \bmod \frac{12}{6}=2$	
$\{0\}$	$\gcd(a,12)=12$	$\{0\} \bmod 1$	

This week

Primitive roots, discrete log, quadratic residues

Primitive Roots

(structure of multiplicative group $\mathcal{U}(p)$)

Recall: p prime $\Rightarrow$ if $a, b \not\equiv 0 \ (p)$ then $ab \not\equiv 0 \ (p)$

$\Rightarrow$ $p-1$ invertible residues: $1, 2, \ldots, p-1$.

Problem: Solve $x^5 \equiv 7 \ (17)$

Method 1: Brute force

Method 2: $\mathrm{ord}_{17}(2) = 8$.

$2^4 \equiv 16 \equiv -1 \ (17)$

$\Rightarrow 2^8 = (2^4)^2 \equiv 1 \ (17)$

Also, $6^2 = 36 \equiv 2 \ (17)$.

Claim: $\mathrm{ord}_{17}(6) = 16$

Pf: Know $6^{16} \equiv 1 \ (17)$ (Fermat's little thm)

If $\mathrm{ord}_{17}(6) < 16$, it's a proper divisor of 16, i.e. a power of 2 with exponent ≤ 3, i.e. a divisor of 8 so if $\mathrm{ord}_{17}(6) < 16$,

$6^8 \equiv 1 \ (17)$ but $6^8 = (6^2)^4 \equiv 2^4 \equiv 16 \equiv -1 \ (17)$

We found 6^{16} $\text{ord}_{17}(6) = 16 = 17-1$

so $\{1 = 6^0, 6 = 6^1, 2 = 6^2, \ldots, 6^{15}\}$ all distinct mod 17

but these are 16 numbers, so these are all the residues mod 17 (except 0)

i.e. mult. gp mod 17 look like additive gp mod 16:

$$6^a \cdot 6^b \equiv 6^{a+b} \quad (\text{take } a+b \bmod 16)$$

(because every residue is a power of 6)

Logarithm table mod 17

$6^4 = 2^1$ $\qquad$ $6^6 = 2^3$

$6^0 \equiv 1,\ 6^1 \equiv 6,\ 6^2 \equiv 2,\ 6^3 \equiv 12,\ 6^4 \equiv 4,\ 6^5 \equiv 7,\ 6^6 \equiv 8,\ 6^7 \equiv 9$

$6^8 \equiv -1,\ 6^9 \equiv -6,\ 6^{10} \equiv -2,\ 6^{11} \equiv -12,\ 6^{12} \equiv -4,\ 6^{13} \equiv -7,\ 6^{14} \equiv -8,\ 6^{15} \equiv -$

$1 \equiv 6^0,\ 2 \equiv 6^{14},\ 3 \equiv 6^{15},\ 4 \equiv 6^4,\ 5 \equiv 6^{11},\ 6 \equiv 6^1,\ 7 \equiv 6^5, \ldots$

Solution of problem: write $x \equiv 6^y$, $y \bmod 16$

We need to solve $x^5 \equiv 7 \ (17)$, i.e.

$$(6^y)^5 \equiv 6^5 \iff 6^{5y} \equiv 6^5 \ (17)$$

$$\iff 5y \equiv 5 \ (16) \quad (\text{ord}_{17}(6))$$

(5 is invertible mod 16)

$$\iff y \equiv 1 \ (16)$$

$$\Rightarrow x \equiv 6^1 \ (17)$$

$$\equiv 6$$

Key tool: The class 6 mod 17 has order $16 = 17-1$ so every non-zero residue was a power of 6 (mod 17)

Can now solve any equation of the form $x^a \equiv b \ (17)$ by writing $x \equiv 6^y$, $b = 6^c$ (get c from table) so the equation becomes

$$6^{ay} = (6^y)^a \equiv b \equiv 6^c \ (17)$$

i.e. $ay \equiv c \ (16)$ ← congruence for power of 6, $\text{ord}_{17}(6) = 16$

(Prop: If $(a,m)=1$ then $a^r \equiv a^s \ (m)$ iff $r \equiv s \ (\text{mod } \text{ord}_m(a))$)

Solve $x^5 \equiv 4 \ (17)$: need to solve $x^5 \equiv 6^4 \ (17)$

write $x \equiv 6^y$, get $6^{5y} \equiv 6^4 \ (17)$ ↖ $\text{ord}_{17}(6) = 16$

$$5y \equiv 4 \ (16)$$

$$\Downarrow$$

$$-15y \equiv -12 \ (16)$$

$$\Downarrow$$

$$y \equiv 4 \ (16)$$

so $x^5 \equiv 4 \ (17)$ iff $x \equiv 6^4 \equiv 4 \ (16)$

Solves $x^6 \equiv 4 \ (17)$

again, $(4, 17) = 1$ so any solution is invertible

so can change variables to $x \equiv 6^y$, $y \bmod 16$. (6 is a primitive root mod 17)

the equation then reads

$$6^{6y} = (6^y)^6 \equiv 4 \equiv 6^4 \ (17)$$

$\Leftrightarrow$

$$6y \equiv 4 \ (16)$$

$\Leftrightarrow$ (divide by 2)

$$3y \equiv 2 \ (8)$$

$\Leftrightarrow$ (mult by $\bar{3} \equiv 3 \ (8)$)

$$y \equiv 6 \ (8)$$

$\Leftrightarrow$

$$y \equiv 6, 14 \ (16)$$

$\Rightarrow$

$$x \equiv 6^6, 6^{14} \ (17)$$

$$\equiv 8, -8 \ (17)$$

Summary: (1) 6 mod 17 has property $\text{ord}_{17}(6) = 16 = \#U(17)$
so every unit mod 17 is a power of 6.
(2) Can use this to solve equations involving powers.

Def: Call a a **primitive root** mod m if $(a,m)=1$ and

$$\text{ord}_m(a) = \phi(m)$$

(recall that $\text{ord}_m(a) \mid \phi(m)$ for any $a \in U(m)$ by Euler)

In that case $U(m) = \{a^j\}_{j=0}^{\phi(m)-1}$

Thm: Let r be a primitive root mod m, b invertible mod m
say $b \equiv r^\ell (m)$
Then the equation $x^n \equiv b \equiv r^\ell \ (m)$ has solutions iff
$(n, \phi(m)) \mid \ell$.

if they exist, there are $(n,\phi(m))$ solutions

Pf: change variables $x \equiv r^y$ then the equation

$x^n \equiv b \ (m)$ becomes

$$r^{ny} \equiv r^\ell \ (m)$$
$$\iff$$
$$ny \equiv \ell \ (\phi(m)).$$

($\phi(m) = \text{ord}_m(r)$)

∎

Cor: b is an nth power iff $(n, \phi(m)) \mid \ell$

$\iff$ $\frac{\phi(m)}{(n,\phi(m))} \ell \equiv 0 \ (\phi(m))$

Def: Let r be a primitive root mod m.
Call the ℓ s.t. $r^\ell \equiv b \pmod m$ the discrete logarithm of b to base r mod m.
(ℓ only defined mod $\phi(m)$)

Fact: Primitive roots exist mod m iff m is of the form
$2, 4, p^k, 2p^k$
where p is an odd prime, $k \geq 1$

Kind of questions we can answer using a primitive root:

(1) solve $x^n \equiv b \pmod m$

(2) Decide if solutions exist (iff $b^{\frac{\phi(m)}{(\phi(m),n)}} \equiv 1 \pmod m$)

no need to find r

Next time: (1) show $\exists$ primitive roots mod p
(2) Diffie-Hellman, El Gamal crypto