Math 312, lecture 24

Recently: RSA: let \( \{ \begin{align*} &m = pq \quad (p, q \text{ prime}) \\ &ed = 1 \quad (\phi(m)) \end{align*} \) \)

Set \( \begin{align*} &E(a) = a^e \pmod{m} \quad \text{for messages} \\ &D(b) = b^d \pmod{m} \quad a, b \in U(m) \end{align*} \)

Can use this for encryption (Bob sends \( b^{E(a)} \) to Alice, she computes \( D(b^{E(a)}) \) to recover \( a \)).

Also for digital signature (Alice signs message \( b \) by publishing \( (b, D(b)) \), anyone can verify this using \( E \).

Road map: We've been calculating in the multiplicative group \( U(m) \) for a while.

1. Invertibility, multiplicative order,
2. Theorems of Fermat and Euler: function \( \phi \)
3. RSA: an application of arithmetic in \( U(m) \)

Next few lectures:
(4) multiplicative group mod p: primitive roots, discrete log, application: Diffie-Hellman, key exchange. [Safe primes will show up!]

(5) squares mod p and quadratic reciprocity

---

**Primitive roots**

Example: Let's solve the congruence \( x^5 \equiv 7 \pmod{17} \) (can brute-force the problem, not good idea)

**Solution 1**: (review of RSA) \( \phi(17) = 17 - 1 = 16 \) and \( 5 \cdot 3 = -1 \pmod{16} \) so \( 5 \cdot 13 \equiv 1 \pmod{16} \).

So if \( x^5 \equiv 7 \pmod{17} \) then \( (x^5)^{13} \equiv 7^{15} \pmod{17} \)

so \( x \equiv 7^{13} \pmod{17} \)

**Solution 2**: in \( \mathbb{R} \), take log, set \( 5 \log x = \log 7 \)

so \( \log x = \frac{1}{5} \log 7 \).

(i.e. we represent \( x \) as \( e^k \), solve for \( k \))
Here, \(2^8 \equiv 1\ (\text{mod } 17)\) so \(2^8 \equiv 1\ (\text{mod } 17)\) so \(\text{ord}_{17}(2) \mid 8\), but \(\text{ord}_{17}(2) \nmid 4\), so \(\text{ord}_{17}(2) = 8\).

(so 2 has 8 distinct powers mod 17)
powers of 2 do not cover \(\mathbb{U}(17)\).

Observe that \(6^2 = 36 \equiv 2\ (\text{mod } 17)\)
\(\therefore 6^8 = (6^2)^4 = 2^8 \equiv 1\ (\text{mod } 17)\)

(i.e. \(\text{ord}_{17}(6) \mid 16\), but we knew that from Fermat's little thm)

\(\therefore\) but \(\text{ord}_{17}(6) \nmid 8\), so \(6^8 \equiv 2^4 \equiv -1\ (\text{mod } 17)\)

\(\therefore\) \(\text{ord}_{17}(6) = 16 = \phi(17)\)

\(\therefore\) 6 has 16 distinct powers mod 17,
i.e. every \(a \in \mathbb{U}(17)\) is of the form \(6^k\),
for a unique \(k\) mod 16

Def: If we have \(a \in \mathbb{U}(m)\) s.t. \(\text{ord}_m(a) = \phi(m)\)
\(\therefore\) every \(a \in \mathbb{U}(m)\) is a power of \(a\)
call a \( a \) a **primitive root** mod \( m \).

**Example:** 2 is a primitive root mod 17.

2 is not a **prim. root** mod 17.

**Back to our problem:** \( x^5 \equiv 2 \pmod{17} \)

Then write \( x = 6^k, \quad 7 = 6^m \).

What is \( m \)? ("discrete log of 7 to base 6,
mod 17")

**Brute-force:**

\[
6^2 \equiv 2, \quad 6^3 \equiv 12, \quad 6^4 \equiv 4, \quad 6^5 \equiv 7.
\]

So if \( x = 6^k \) have \((6^k)^5 = 6^5 \pmod{17} \)

so \( 5k \equiv 5 \pmod{\phi(17)} \) \( \Rightarrow k \equiv 1 \pmod{16} \)

\( \Rightarrow x \equiv 6 \pmod{17} \)

Similarly, to solve \( x^5 \equiv 4 \pmod{17} \),
write this as \((6^k)^5 = 6^4 \pmod{17} \)

so \( 5k \equiv 4 \pmod{16} \) \( \Rightarrow k \equiv 4 \pmod{16} \)
80 \ k = 6^4 = 6^8 = 4 \quad \text{and indeed}

4^5 = 4 \quad (17)

---

Find some primitive roots

\text{mod 17:} \ 6 \ \text{is, \ 2 \ isn't.}

\text{mod 19:} \ \text{ord}_{19}(2) \mid 18, \ \text{if not 18 \ it would divide 9 or 6.}

2^3 = 8, \quad 2^6 = 64 = 7 \quad (19)

2^9 = 7 \cdot 8 \equiv 86 = -1 \quad (19)

\text{so \ \text{ord}_{19}(2) = 18 = \phi(19)}

(2 \ is \ a \ primitive \ root)

Again, this means \ \text{U}(17) = \{ 6^i \}_{i=0}^{15}

\text{U}(19) = \{ 2^j \}_{j=0}^{14}

no primitive root mod 8: \ \text{even \ a \in U}(8)
Let $a^n = 1 \mod m$ for some $a$ and $n$. The powers of $a$ are just $1, a, a^2, \ldots$.

**Theorem:** ("discrete log") Let $r$ be a primitive root mod $m$. Then the congruence

$$x^n \equiv r^l \mod m$$

has solutions iff $(n, \phi(m)) \mid l$. In that case, there are $(n, \phi(m))$ solutions.

**Proof:** will show: $b \in \mathbb{U}(m)$ is an $n$th power mod $m$ iff $b^{(n, \phi(m))} \equiv 1 \mod m$,

then $b$ has $(n, \phi(m))$ $n$th roots.

**Pf:** Can write $x \equiv r^b \mod \phi(m)$ [use that $r$ is a primitive root]

then need to solve $r^{nt} \equiv r^l \mod m$.

This is equivalent to $nt \equiv l \mod \phi(m)$.

i.e. $nt = l$ (mod $\phi(m)$).
That's a linear congruence. (unknown is \( t \))

let \( d = (n, \phi(m)) \). Then \( d \mid nt \), and if \( t \) is a solution \( l \equiv nt \pmod{d} \)
so \( l \equiv 0 \pmod{d} \)
so if \( d \mid l \), no solutions

On the other hand, if \( d \nmid l \), then

\[
nt \equiv l \pmod{\phi(m)}
\]

\[
\frac{n \cdot t}{d} \equiv \frac{l}{d} \pmod{\frac{\phi(m)}{d}}
\]

now \( (\frac{n}{d}, \frac{\phi(m)}{d}) = 1 \) so this has a unique solution mod \( \frac{\phi(m)}{d} \). But every class mod \( \frac{\phi(m)}{d} \) is the union of \( d \) classes mod \( \phi(m) \)
so have \( d \) solutions to \( nt \equiv l \pmod{\phi(m)} \).

When is \( b \) an \( n \)-th power? if it is, the congruence \( nt \equiv l \pmod{\phi(m)} \) has solution \( d \) mod
\[ x \in \mathbb{Z} \] need not always have a \( d \)-th power \( n^d \equiv b \pmod{m} \) of them

\[ \frac{n}{d} \text{ invertible mod } \phi(m) \]

- if \( x^n \equiv b \pmod{m} \) then

\[ b^{\frac{\phi(m)}{d}} \equiv (x^{\frac{n}{d}})^{\phi(m)} \equiv 1. \]

Today: explored idea of primitive roots
residues \( r \equiv \Phi(n) \) mod \( m \), such that \( \exists r \in U(m) \equiv \text{ord}_m(r) = \phi(m) \)

Next time: Applications, safe primes
(aside: always a primitive root mod \( p \))
Proof next Friday.