Previously in Math 103a

Thm 1 s, t coprime $\Rightarrow$

$$\boxed{U(st) \approx U(s) \oplus U(t)}$$

with isomorphism given by

$$x \longmapsto (x \bmod s,\ x \bmod t).$$

Ex. $U(120) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 + \mathbb{Z}_4$

Reason: $120 = 12 \times 10 = 2 \times 2 \times 3 \times 2 \times 5$

$= 8 \times 3 \times 5$

$\therefore U(120) \approx U(8) \oplus U(3) \oplus U(5)$

$U(8) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$ we checked this earlier!

$|U(3)| = 2 \Rightarrow U(3) \approx \mathbb{Z}_2$

$U(5) = \{1, 2, 3, 4\}$ cyclic order 4

$\therefore U(5) \approx \mathbb{Z}_4$

Thm 2 If p is prime, then $U(p)$ is cyclic.

Outline of proof. By contradiction, if $\exists$ no element of order $p-1$, then can show $\exists\ m < p-1$ s.t. $x^m \bmod p = 1$ $\forall\ x \in U(p)$. This gives $p-1$ roots to the equation $x^m - 1 = 0$ in $U(p)$, which should have at most m roots. Important details missing here!

Thm 3 If $x \in U(p)$ is a generator (which exists by the previous Thm), then $U(p) \approx \mathbb{Z}_{p-1}$, and an isomorphism is given by

$$\Phi(x^k) = k, \quad k = 0, 1, \ldots p-2$$

for $x = 1, 2, \ldots, p-1$ in $U(p)$.

Pf: Since x is a generator of $U(p)$, an isomorphism is determined by

$\Phi(x) = j$, where j is any generator of $\mathbb{Z}_{p-1}$

since Φ preserves multiplication

$$\Phi(x^k) = \Phi(\underbrace{x\, x \cdots x}_{k}) = \underbrace{\Phi(x) + \Phi(x) + \cdots + \Phi(x)}_{k}$$

$$= k \cdot j$$

Thm 4. If p & q are primes, $p \neq q$, then

$$U(pq) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}.$$

Pf Since p & q are coprime,

$$U(pq) \approx U(p) \oplus U(q) \underset{\text{by previous Thm}}{\approx} \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}$$

Application to public key cryptography.

Problem: How can Person A publish a public method for sending a message to A that only A can decipher. That is, the method for scrambling a message is known, but method for unscrambling is not known (except by A).

Idea: find some one way computation.

Method (RSA) Convert the message into a string of digits, e.g. use 01 for A, 02 for B, etc. Then divide the string into blocks of say 4 digits.

Person A chooses 2 very large prime numbers p & q. Then pick a number $r > 0$ such that $\text{lcm}(p-1, q-1)$ is coprime to r.

Put $n = pq$ and publish the pair (n, r) as a "public key" for A.

To describe encoding, we'll follow example in text:

Take $p = 37$, $q = 73$, $r = 5$

$\text{lcm}(p-1, q-1) = 72$

Now suppose person B wants to send the message (2505, 1900) to A.

Each block needs to be scrambled. (It is important that each number is < 2701.)

The coded message $= ((2505)^5 \bmod 2701,$
$(1900)^5 \bmod 2701)$

$(2505)^5 \bmod 2701 = 2415$

(This can be calculated one power at a time e.g. $(2505)^2 \bmod 2701$, etc.)

Person A receives the message. To decode, use the inverse of $5 \bmod \text{lcm}(p-1, q-1)$. Since $\gcd(5, 72) = 1$,

$\exists\ s, t$ with $5s = 1 + 72t$

Can take $s = 29$.

(This cannot be found without knowing $p-1, q-1$)

Then $(2415)^{29} \bmod 2701 = 2505$

Amazing!

Why does it work?

$(2415)^{29} \bmod 2701 = \left((2505)^5\right)^{29} \bmod 2701$

(since $s=29$) $= (2505)^{1+72t} \bmod 2701$

$= (2505)(2505)^{72t} \bmod 2701$

We just need to know $(2505)^{72} \bmod 2701 = 1$

Our data: $2701 = pq$, p, q prime

here $p=37$, $q=73$

Claim: p, q prime, $m = \text{lcm}(p-1, q-1) \Rightarrow$

$$\boxed{x^m \bmod pq = 1}$$

for any $0<x<p$ & $x<q$, or,

more generally, any x satisfying $\gcd(x,p) = \gcd(x,q) = 1$.

Pf: $x \in U(pq)$ by assumption.

$U(pq) \approx U(p) \oplus U(q)$, by isomorphism

$x^m \longmapsto (x^m \bmod p, x^m \bmod q)$

$= (x_1^{j_1 m} \bmod p, x_2^{j_2 m} \bmod q)$

where x_1 is a generator of $U(p)$
& x_2 is a generator of $U(q)$

Now apply the isomorphism given by

Thm 3 $\quad U(p) \oplus U(q) \to \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}$

to get $(x_1^{j_1 m} \bmod p-1,\ x_2^{j_2 m} \bmod q-1)$

$\longmapsto (u_1 m \bmod p-1,\ u_2 m \bmod q-1)$ **

for some integers u_1, u_2

Since $p-1 \mid m$ & $q-1 \mid m$

The RHS of (**) is $(0,0)$, the identity in $\mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}$.

An isomorphism takes the identity to identity (and is 1-1)

$\therefore x^m \bmod pq = 1$, the identity in $U(pq)$.

We'll accept without proof!

Thm. If p is an odd prime, then

$$U(p^k) \approx \mathbb{Z}_{p^k - p^{k-1}}$$

$$U(2^k) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{k-2}}$$

Now we can decompose any $U(m)$!