In this lecture we go into a bit more detail about residue structures. These notes closely follow Evan Chen’s notes at https://web.evanchen.cc/handouts/CRT/CRT.pdf and https://web.evanchen.cc/handouts/ORPR/ORPR.pdf.

Last time we left off at the CRT, which states that if \((x,y) = 1\) (the greatest common divisor of \(x\) and \(y\) is 1), then there is a bijection between \(a \mod x\), \(a \mod y\), and \(a \mod xy\). We begin with a few more uses of it.

**Problem 1.1.** Let \(n\) be a positive integer and let \(a_1, a_2 \ldots a_k\) \((k \geq 2)\) be distinct integers with \(1 \leq a_i \leq n\) such that

\[ n \mid a_i (a_{i+1} - 1) \quad 1 \leq i \leq k - 1. \]

Prove that \(n\) does not divide \(a_k(a_1 - 1)\).

By CRT, we consider the case where \(n = p^e\) for some prime \(p\). Let \(x_i\) be the max power of \(p\) that divides \(a_i\), and \(y_i\) the max power of \(p\) that divides \(a_i - 1\). Note that because \((a_i, a_i - 1) = 1\), either \(x_i\) or \(y_i\) must be 0.

Suppose by contradiction we do have \(p^e | a_i(a_{i+1} - 1)\) (overloading indices to let index \(n + 1\) loop back to 1). Then for each \(i\) we have \(x_i + y_{i+1} \geq e\). If \(x_1 \geq 0\), then we get \(y_1 = 0\), which by the last equation implies \(x_k \geq e\), and in turn \(y_{k-1} = 0\) and \(x_{k-1} \geq e\). So inductively we’d get \(x_i \geq e\). Alternatively, we’d get all \(y_i \geq e\).

This means that each \(a_i\) must either be \(0 \mod p^e\), or \(1 \mod p^e\). Putting these prime powers back together then gives a contradiction to the \(a_i\)s being distinct.

Now for something more intricate:

**Problem 1.2.** Prove that for every integer \(n\), there are pairwise relatively prime integers \(k_1 \ldots k_n\), each greater than 1, such that \(k_1 \cdot k_2 \ldots \cdot k_n - 1\) is the product of two consecutive integers.

The problem is equivalent to finding

\[ x (x + 1) \equiv 1 \pmod{k_i} \]

for all \(1 \leq i \leq n\).

We first show that there are infinitely many \(p\) for which the equation

\[ x (x + 1) \equiv 1 \pmod{p} \]

...
has a solution. Suppose not, let the total number of such primes be \( n \). For some value \( L \) which we will use to give a contradiction, consider all products \( x(x + 1) \) for \( x \) between \( 1 \ldots 2^L \). The number of products of exponents of these \( n \) primes is at most 
\[
L^{2n},
\]
because each can be taken to power at most \( 2n \), while the number of products is \( 2^L \). Letting \( L \) growing much more than \( n \) gives a contradiction, as \( 2^L \) is exponential, \( L^{2n} \) is polynomial (here \( n \) is treated as a constant: this is ok because we are picking \( L \) after picking \( n \)).

So we can find \( n \) primes \( p_1 \ldots p_n \) such that for each \( p_i \), we have some \( x_i \) s.t.
\[
x_i (x_i + 1) \equiv 1 \pmod{p_i}.
\]

By CRT, we can find some \( x \) s.t. \( x(x + 1) \equiv 1 \pmod{p_i} \) for all \( i \).

Informally, CRT essentially says that \( \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \) basically behaves like \( \mathbb{Z}_{p_1 \times p_2} \). This is informal: formalizing CRT in abstract algebra one needs ideals, which I don’t plan to cover in this class.

In the rest of this lecture, I want to discuss the multiplicative structure modulo \( p \) in a bit more detail. The main idea is that everything from \( 1 \ldots p - 1 \) can be written as
\[
g^x \mod p
\]
for some \( g \) that we refer to as the generator.

This representation may seem strange. I was first convinced of its utility via the following fact about quadratic residues

**Fact 1.3.** Let \( p \) be an odd prime. There exists some \( a \) such that
\[
a^2 \equiv -1 \pmod{p}
\]
if and only if \( p \equiv 1 \pmod{4} \).

Because \((-1)^2 = 1\), for this generator, we must have
\[
-1 \equiv g^{\frac{p-1}{2}} \pmod{p}
\]
The ‘root’ of \(-1\) is then \( g^{\frac{p-1}{2}} \).

For this to exist, \( p - 1 \) must be a multiple of 4.

So we want to show that generators do exist modulo \( p \). We denote the order of some value \( x \mod p \) to be the smallest \( e \) such that
\[
x^e \equiv 1 \pmod{p}
\]
The following sequence of steps then allows us to conclude the existence of generators:
1. If \( x^{e_1} \equiv 1 \pmod{p} \) and \( x^{e_2} \equiv 1 \pmod{p} \), then \( x^{(e_1,e_2)} \equiv 1 \pmod{p} \).

2. For any \( x \), \( \operatorname{ord}(x)|(p-1) \). This is by combining step (1) with \( x^{p-1} \equiv 1 \pmod{p} \).

3. For each divisor \( d \) of \( p \), there are at most \( \phi(d) \) elements with order \( d \). Here \( \phi(d) \) is the Euler totient function of \( d \), aka. the number of numbers between 1 and \( d-1 \) that are relatively prime to \( d \).

The bound of at most \( d \) is a direct implication of Lagrange's theorem / Schwarz-Zippel, which states a non-zero degree \( d \) polynomial has at most \( d \) roots modulo a prime \( p \). This lemma is in turn proven using polynomial division (we will revisit this later).

4. For any \( m \), we have
   \[
   \sum_{d|m} \phi(d) = m,
   \]
   so there must be terms with order \( p-1 \).

We will discuss how generators broke algorithm design over the next two weeks. For this class though, we will just stop by yeeting an IMO #6 with generators and orders.

**Problem 1.4.** Let \( p \) be a prime number. Show that there is a prime \( q \) such that for all integers \( n \), we have

\[
q \not| n^p - p
\]

By generators, we have

\[
p \equiv g^e \pmod{q}
\]

for some integer \( e \). If \((p,q-1) = 1\), we can ‘divide’ \( e \) by \( p \) and set \( n \leftarrow g^{e/p} \). So we must have

\[
p \mid q - 1.
\]

Let \( q = pk + 1 \).

Then because for any \( n \), we have

\[
1 \equiv n^{q-1} \equiv n^{pk}
\]

a sufficient condition for \( q \) is

\[
p^k \not\equiv 1 \pmod{q}.
\]

The ‘magic’ step is to take \( q \) to be a prime factor of

\[
\frac{p^p - 1}{p-1} = \sum_{i=0}^{p-1} p^i.
\]

The overall product has residue \( 1+p \) modulo \( p^2 \), so we can choose \( q \) to be not 1 modulo \( p^2 \). Now observe that:

1. \( p \) has order \( p \) modulo \( q \) by construction. This implies \( p|q-1 \).

2. \( k \) is not a multiple of \( p \), since otherwise \( q = kp + 1 \) would be 1 mod \( p^2 \).