CS174 Spr 99 Lecture 23 Summary John Canny

More Number Theory

From last time we know that the order of a subgroup $H \subseteq G$ divides the order of the group. We also know that for any element $a \in G$, the order of the element $\mathrm{ord}(a)$ equals the order of the subgroup generated by a which is $\{a, a^2, \ldots, a^{\mathrm{ord}(a)} = 1\}$. Therefore

Proposition 1
The order of an element $\mathrm{ord}(a)$ divides the order of the group G and so

$$a^{|G|} = 1$$

This follows because $\mathrm{ord}(a) = |H|$ where H is the subgroup generated by a. Therefore

$$a^{|H|} = a^{\mathrm{ord}(a)} = 1$$

And since $|H|$ divides $|G|$, $|G| = m|H|$ for some integer m. So

$$a^{|G|} = \left(a^{|H|}\right)^m = (1)^m = 1$$

The above results are general. Even though they seem to be written for multiplication, dont forget that they apply to the group operation $\cdot$. So for $\mathbb{Z}_p$ they apply to both addition and multiplication.

Let's try to figure out the order of an element in the *additive* group $(\mathbb{Z}_p, +)$. The additive identity is zero, so this is the same question as asking how many times we can add the element to itself before we generate zero $(\mathrm{mod}\ n)$, i.e. how many times can we add the element to itself before generating a multiple of n for the first time:

$$\mathrm{ord}(a) \times a = kn$$

which is the same as asking for the LCM of a and n. We already know how to express the LCM in terms of the GCD of a and n. Doing that gives the following proposition:

Proposition 2
Let $\mathrm{ord}(a)$ be the order of a in the additive group $(\mathbb{Z}_n, +)$. Then

$$\mathrm{ord}(a) = \frac{\mathrm{lcm}(a, n)}{a} = \frac{n}{\gcd(a, n)}$$

For the multiplicative group $(\mathbb{Z}_n^*, \times)$, remember that the number of elements in the group is given by Euler's totient function $\phi(n)$. By proposition 1, it follows that:

Euler's Theorem For any element $a \in \mathbb{Z}_n^*$,

$$a^{\phi(n)} = 1 (\bmod\ n)$$

For a prime p, recall that $\phi(p) = p - 1$. Making that substitution gives us Fermat's theorem (not the famous one):

Fermat's Theorem For a prime p and any element $a \in \mathbb{Z}_p^*$,

$$a^{(p-1)} = 1 (\bmod\ p)$$

Fast Powering

You might remember the efficient algorithm for powering (from CS170). To compute a^n, you can use the following pseudo-code:

```
Algorithm FastPower(a, n)
  if (n == 0) return 1
  elseif (n == 1) return a
  else
    temp = FastPower(a, floor(n/2))
    temp = temp * temp
    if (odd(n)) temp = temp * a
    return temp
end
```

It should be fairly easy to see that the recursion depth (and the running time) is proportional to $\log n$. Arithmetic $(\bmod\ n)$ also takes time that is polynomial in $\log n$. So e.g. its possible to compute

$$a^{(p-1)} (\bmod\ p)$$

in time which is polynomial in $\log p$.

Generators

Recall that a generator of a group G is an element whose powers comprise the entire group G. If a group has a generator, then it is said to be a **cyclic** group. One easy observation we can make is that if the order of G is a prime $p > 1$, then G is a cyclic group. Why? Because the order of every element divides the order of G. Since the order of G is p, every element has order 1 or p. In the first case it must be the identity (the only element with order 1), and in the second case its order equals the order of the group, so it is a generator. In fact every element except the identity is a generator.

In particular, for every prime p, the additive group $(\mathbb{Z}_p, +)$ is cyclic. Its order is p, and every element except 0 generates the whole group.

For multiplicative groups, we dont get very far with the above observation. For prime p, the order of $(\mathbb{Z}_p^*, \times)$ is $p-1$. If p is prime and greater than 2, it must be odd, and $p-1$ must be even. That is, the order of $(\mathbb{Z}_p^*, \times)$ for $p > 2$ is divisible by 2. So we can't apply the above theorem. But that doesnt mean that $(\mathbb{Z}_p^*, \times)$ is not cyclic. In fact it always is:

Theorem The multiplicative group $(\mathbb{Z}_n^*, \times)$ is cyclic if and only if n is either:

$$1,\ 2,\ 4,\ p^k,\ \text{or } 2p^k$$

where p is an odd prime, and k is a positive integer.

This theorem is quite complicated to prove, and we wont do that here. It is anyway not all that interesting to know that a group is cyclic (has a generator). What is interesting is if there are *lots of* generators. In fact, that is the case for cyclic groups. Once you have a generator, many powers of that generator will also be generators.

Lemma If g is a generator of $(\mathbb{Z}_n^*, \times)$, then so is g^k so long as $\gcd(k, \phi(n)) = 1$.

Proof
Let $h = g^k$. Then h is a generator unless there is an $m < \phi(n)$ such that

$$h^m = 1 (\bmod\ n)$$

Suppose such an m exists (i.e. suppose h not a generator). Then

$$(g^k)^m = g^{(km)} = 1 (\bmod\ n)$$

which implies that km is a multiple of $\phi(n)$, because $\phi(n)$ is the smallest power of g which is 1 $(\bmod\ n)$. Since k has no shared factors with $\phi(n)$ (their gcd is 1), that means that m must be a multiple of $\phi(n)$. But that contradicts our assumption that $m < \phi(n)$. So h as defined above must be a generator.

This lemma shows that there are at least as many generators for a cyclic group $(\mathbb{Z}_n^*, \times)$ as there are integers k which are less than and relatively prime to $\phi(n)$. Those k values are precisely the elements of $\mathbb{Z}_{\phi(n)}^*$, and there are $\phi(\phi(n))$ of them.

To recap, if the multiplicative group $(\mathbb{Z}_n^*, \times)$ is cyclic, then at least $\phi(\phi(n))$ of its elements are generators. The multiplicative group itself has $\phi(n)$ elements, so the fraction of elements which are generators is $\phi(\phi(n))/\phi(n)$. This is a clumsy expression. If we define $N = \phi(n)$ as the order of the group, then the fraction of generators is $\phi(N)/N$. The following lemma shows that this ratio isnt too small:

Lemma For any $N > 1$,

$$\frac{\phi(N)}{N} = \Omega\left(\frac{1}{\log N}\right)$$

Proof

From our earlier discussion, we know that if N has a prime-power factorization as $p_1^{k_1} \cdots p_t^{k_t}$, then

$$\phi(N) = N \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right)$$

Since each prime factor is at least 2, the number of distinct factors t of N is at most $\log_2 N$.

Next notice that the value of the product increases with p_i. That is, if we increase p_i, then $(1 - 1/p_i)$ increases. So if we have another sequence of numbers $q_1, \ldots, q_t$ where $p_i > q_i$ for all i, then

$$\prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) > \prod_{i=1}^{t} \left(1 - \frac{1}{q_i}\right)$$

Suppose we order the distinct primes p_i's in increasing order $p_1 < p_2 < \cdots < p_t$. Then a suitable sequence of q_i's would be $1, 2, 3, 4, 5, \ldots, t$. Each q_i will be less than p_i. The product

$$\prod_{i=1}^{t} \left(1 - \frac{1}{q_i}\right) = \frac{1}{2}\frac{2}{3}\frac{3}{4} \cdots \frac{t-1}{t} = \frac{1}{t} \geq \frac{1}{\log_2 N}$$

So we have shown that

$$\phi(N)/N = \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) > \prod_{i=1}^{t} \left(1 - \frac{1}{q_i}\right) \geq \frac{1}{\log_2 N}$$

which completes the proof.

The reason that is so interesting is that for a cyclic group like $(\mathbb{Z}_p, \times)$, at least $1/\log p$ of the elements will be generators (actually at least $1/\log N$ which is at least $1/\log p$ because $N = \phi(p) < p$). So if we pick elements at random, we only need to make about $O(\log p)$ guesses before we have a good chance of getting a generator. We can do quite a few interesting things with generators. For example, we can prove that p is prime even if we didnt know in advance that it is, by showing that the generator has order $p - 1$. The above results show that we can do this, and hence discover large primes, in time polynomial in $\log p$.