Lecture 01

Jose Capco (jcapco@risc.jku.at)

Polynomial Division. Let R be a non-trivial commutative ring

1. If $f, g \in R[X]$ and g is monic and not zero then there are unique $q, r \in R[X]$ such that $f = gq + r$ with $\deg(g) < \deg(r)$.
2. If $f \in R[X]\backslash\{0\}$ and $a \in A$ then there is a unique $g \in R[X]$ such that $f = (X - a)g + f(a)$. Thus, if $a \in A$ is a zero of f then $(X - a) \mid f$.
3. If R is a domain and $a_1, a_2, \ldots, a_k \in A$ are distinct zeros of $f \in R[X]\backslash\{0\}$, then

$$\prod_{i=1}^{k}(X - a_i) \mid f$$

   Thus, f cannot have more zeros than $\deg(f)$

Proof. 1 Existence is clear. We prove uniqueness. Suppose that $q, q', r, r' \in R[X]$ exists such that

$$f = gq' + r' = gq + r$$

If $q - q' \neq 0$ then

$$\deg(g) + \deg(q - q') \geq \deg(g) > \deg(r - r')$$

and this contradicts $g(q - q') = r - r'$.

2 We substitute g above with $X - a$ then for r above we have $\deg(r) < \deg(g)$ so $r \in R$. Substituting the indeterminate X with a in division with remainder above solves $r = f(a)$. The second statement is then clear.

3 This can be proven by induction. First induction step comes from 2. Suppose now that $k > 1$ and $g = \prod_{i=1}^{k-1}(X - a_i)$ with $g \mid f$. Because a_i are distinct for $i = 1, \ldots, k$ and because R is an integral domain, we have $g(a_k) \neq 0$. Also since $g \mid f$ we have $gq = f$ for some $q \in A[X]$. Because $g(a_k) \neq 0$ and we are in a domain, we have

$$g(a_k)q(a_k) = f(a_k) = 0 \Rightarrow q(a_k) = 0$$

which by 2 implies that $(X - a_k) \mid q$ i.e. $q = (X - a_k)q'$ for some $q' \in A[X]$. □

Exercise 1. In the Theorem above

- Show that 3 does not hold if we remove the condition that R is a domain.
- Show that 2 does not hold if we remove the condition that R is commutative.

Lemma 1. Let G be a group and suppose $g, h \in G$ with $gh = hg$ and $\mathrm{ord}(g), \mathrm{ord}(h)$ finite.

1) If $\mathrm{ord}(g)$ is coprime with $\mathrm{ord}(h)$ then $\mathrm{ord}(gh) = \mathrm{ord}(g)\,\mathrm{ord}(h)$.

2) There exists a $g' \in G$ such that $\mathrm{ord}(g') = \mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(h))$

Proof. Set $m := \mathrm{ord}(g), n := \mathrm{ord}(h)$ let 1 be the identity element in G.

1) Set $k := \mathrm{ord}(gh)$, then since $(gh)^{mn} = 1$ we get $k \mid mn$. Consider now $p \in \mathbb{P}$ such that $p^\nu \mid m$ but $p \nmid n$ (since m and n are coprime) for some $\nu \in \mathbb{N}$. We claim that p^ν divides k. Let $p^\mu \mid k$ for some $\mu \in \mathbb{N}_0$. Clearly $\nu \geq \mu$, suppose that $\nu > \mu$. Set $l := \nu - \mu$, then (because $k \mid \frac{m}{p^l}n$ and $g^n = 1$)

$$(gh)^{\frac{m}{p^l}n} = 1 = g^{\frac{m}{p^l}n} \Rightarrow \mathrm{ord}(g) \mid \frac{m}{p^l}n$$

i.e. $m \mid \frac{m}{p^l}n$, but this implies that $p \mid n$ which is a contradiction (because m and n are coprime). Similar argument holds for primes dividing m but not n. Thus, the prime decomposition of k and mn are the same which implies its equality.

2) If we set $k := \gcd(m,n)$ we see that $k \mid mn$ since $(gh)^{mn} = 1$. Let $k = \gcd(m,n)$ then $\gcd(\frac{m}{k}, n) = 1$ and

$$\operatorname{lcm}(m,n) = \operatorname{lcm}(\frac{m}{k}, n) = \frac{m}{k}n$$

Moreover, we have $\operatorname{ord}(g^k) = \frac{m}{k}$ and so we can use 1) to conclude that

$$\operatorname{ord}(g^k h) = \frac{m}{k}n = \operatorname{lcm}(m,n)$$

□

Proposition 2. Let K be a field then any finite subgroup of K^* is cyclic.

Proof. Let $G \leq K^*$ be a finite subgroup of the multiplicative group of K. Consider the number

$$n := \max\{k \in \mathbb{N} : g^k = 1 \text{ for some } g \in G\}$$

Then we have a $g \in G$ such that $\operatorname{ord}(g) = n$ and clearly $|G| \geq n$. Let $h \in G$ be chosen arbitrarily and set $m := \operatorname{ord}(h)$, then by Lemma 12) there is a $g' \in G$ such that $\operatorname{ord}(g') = \operatorname{lcm}(m,n)$. This implies that $\operatorname{ord}(h) \mid n$ for any $h \in G$. Therefore, any element $h \in G$ is a root of the polynomial $X^n - 1 \in K[X]$. By Polynomial Division 3 we get $|G| \leq n$ and thus the Proposition is proven (with g as the generator of the cyclic group G). □

We now recall some definitions and facts in elementary number theory without providing the proof.

Definition.

- Let $n \in \mathbb{N}$ then an element $a \in \mathbb{Z}$ is called a *quadratic residue mod n* if there is an $x \in \mathbb{N}$ such that $x^2 = a \bmod n$ (i.e. a is a square mod n).
- Let $p \in \mathbb{P}\backslash\{2\}$ and $a \in \mathbb{Z}$ then define the *Legendre symbol (of a mod p)*

$$\left(\frac{a}{p}\right)_L := \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a qaudratic residue mod } p \\ -1 & \text{otherwise} \end{cases}$$

- Let $n \in \mathbb{P}$ and $a \in 2\mathbb{N}_0 + 1$ and write the prime factorization $n = \prod_{i=1}^k p_i^{e_i}$ for finitely many distinct $p_i \in \mathbb{P}$ with $e_i \in \mathbb{N}$. We define the *Jacobi symbol (of a mod n)*

$$\left(\frac{a}{n}\right)_J := \prod_{i=1}^k \left(\frac{a}{p_i}\right)_L^{e_i}$$

The number 2 is not very interesting when studying quadratic residues. So we can henceforth just use the Jacobi symbol for odd numbers (including the primes).

Gauss' Quadratic Reciprocity Laws. Let $p \in \mathbb{P}\backslash\{2\}$, $m, n \in 2\mathbb{N}+1$ and $a, b \in \mathbb{N}$ then we have

- Multiplicative with First Argument: $\left(\frac{ab}{n}\right)_J = \left(\frac{a}{n}\right)_J \left(\frac{b}{n}\right)_J$
- Euler's Criterion: $a^{(p-1)/2} = \left(\frac{a}{p}\right)_L \bmod p$
- First Supplement to QRL:

$$\left(\frac{-1}{n}\right)_J = (-1)^{(n-1)/2} = \begin{cases} 1 & \text{if } n = 1 \bmod 4 \\ -1 & \text{if } n = 3 \bmod 4 \end{cases}$$

- Second Supplement to QRL:

$$\left(\frac{2}{n}\right)_J = (-1)^{(n^2-1)/8} = \begin{cases} 1 & \text{if } n = \pm 1 \bmod 8 \\ -1 & \text{if } n = \pm 3 \bmod 8 \end{cases}$$

- Multiplication of Reciprocals: If $(m, n) = 1$ then

$$\left(\frac{m}{n}\right)_J \left(\frac{n}{m}\right)_J = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

Exercise 2. Write a computer program that takes $a \in \mathbb{N}$ and $n \in 2\mathbb{N}+1$ and outputs the Jacobi symbol $\left(\frac{a}{n}\right)_J$. Hint: Use quadratic reciprocity laws and factorize $a = 2^s t$ where t is odd.

Definition. Let $n \in \mathbb{N}$ with $n > 1$, then we say that $x \in \mathbb{N}$ is a *primitive root mod* n iff $(\mathbb{Z}/m)^*$ is cyclic and is generated by x mod n.

By the Proposition 2, the multiplicative group of the field $(\mathbb{Z}/p)$ is a cyclic group. There is a naive algorithm to check if an element in $1, \ldots, p-1$ is a primitive root mod p ...

Algorithm 1: Find the primitive root mod p

Input: An odd prime p
Output: A number a in $2, \ldots, p-1$ such that a is a primitive root mod p

```
1 Find all distinct primes p_1, p_2, ..., p_k dividing p - 1
2 for a = 2, ..., p - 1 do
3 |  if for all i = 1, ..., k
  |                          a^{(p-1)/p_i} ≠ 1 mod p
  |   then
4 |  |  return a
5 |  end
6 end
```

This is based on the following Proposition which follows immediately by Lagrange's theorem.

Proposition 3. Let p be a prime, then an element $a \in \{1, \ldots, p-1\}$ is a primitive root mod p iff $a^{(p-1)/q} \neq 1 \bmod p$ for every prime divisor q of $p-1$.

One time consuming part in the above algorithm is the factorization of $p-1$ which we will deal with in another lecture.

But for which $n \in \mathbb{N}$ is $(\mathbb{Z}/n)^*$ cyclic? The theorem below says that $(\mathbb{Z}/p^k)^*$ is cyclic for any odd prime p.

Theorem 4. Suppose $p \in \mathbb{P}$ then

1. $n \in \mathbb{N}$ is a primitive root mod p iff n or $n+p$ is a primitive root mod p^2
2. If $p \in \mathbb{P}$ is odd and $k \geq 2$ then $n \in \mathbb{N}$ is a primitive root mod p^k iff n is a primitive root mod p^2

Proof. 1. One easily checks that if $p = 2$ this holds. So we assume without loss of generality that p is an odd prime. One side of the proof is clear, so let us assume $x = 1, \ldots, p-1$ is a primitive root mod p. Let $G := (\mathbb{Z}/p^2)^*$, then we know that $|G| = \phi(p^2) = p(p-1)$ so it suffices to find an element of G of order $p(p-1)$. Now the order of x modulo p^2 should divide $p(p-1)$. Clearly $x^p \neq 1 \bmod p^2$ (otherwise $x^p = 1 \bmod p$ and so x cannot be a primitive root mod p). If $x^{p-1} \neq 1 \bmod p^2$ then we are done. Otherwise, choose $y = x + p$ and here again $y^p \neq 1 \bmod p^2$ and we will prove that $y^{p-1} \neq 1 \bmod p^2$. We then have

$$y^{p-1} = (x+p)^{p-1} = x^{p-1} + (p-1)px^{p-2} = x^{p-1} - px^{p-2} = 1 - px^{p-2} \bmod p^2$$

and this cannot be 1 mod p^2. Thus y has order $|G|$ which means that G is cyclic.

2. This can be proven by induction for $k \geq 2$. The induction hypothesis starts with $k = 2$ which holds by 1. So let us assume that for any number smaller than some $k \geq 2$ the result holds. Let $x \in 1, \ldots, p^2$ be primitive root mod p^2 and for any $n \in \mathbb{N}$ we define the group $G_n := (\mathbb{Z}/p^n)^*$. We want to prove that G_{k+1} is cyclic and generated by x. It suffices to show that

$$x^{p^{k-1}(p-1)} \neq 1 \bmod p^{k+1}$$

We have the following facts:

- x is a generator of G_k, so $x^{p^{k-2}(p-1)} \neq 1 \bmod p^k$
- x is a generator of G_{k-1}, so $x^{p^{k-2}(p-1)} = 1 \bmod p^{k-1}$. This also holds for $k = 2$

Thus, we may write $x^{p^{k-2}(p-1)} = 1 + ap^{k-1}$ for some $a \in \mathbb{N}$ such that $p \nmid a$. We just have to apply binomial expansion to get

$$x^{p^{k-1}(p-1)} = (1 + ap^{k-1})^p = 1 + ap^k \bmod p^{k+1}$$

and see that this cannot be 1 mod p^{k+1}. □

So it suffices to know a primitive root modulo p^2 to know any primitive root modulo p^k. The difficulty then really boils down into finding primitive roots modulo a prime.

We remark (without proof) that $(\mathbb{Z}/n)^*$ is cyclic iff n is one of the following :

- $n = 2$
- $n = 4$
- $n = p^k$ for some $k \in \mathbb{N}$ and odd prime $p \in \mathbb{P}$
- $n = 2p^k$ for some $k \in \mathbb{N}$ and odd prime $p \in \mathbb{P}$

We may as well state an unsolved problem in number theory ...

Artin's Conjecture. Let $a \in \mathbb{N}$ such that a is not a perfect square, then

$$\#\{p \in \mathbb{P} : a \text{ is a primitive root mod } p\} = \infty$$

i.e. there are infinitely many primes p, for which a is a primitive root mod p.

Exercise 3.

1. Prove that for an odd prime p and for $k \in \mathbb{N}$ the multiplicative group $(\mathbb{Z}/2p^k)^*$ is cyclic.
2. Write a program that finds the primitive root mod n if $(\mathbb{Z}/n)^*$ is cyclic.
3. Write a method `ArtinCounts`(a, x) that takes a non-square $a \geq 2$ and $x \in \mathbb{N}$ and counts all prime numbers $p \leq x$ for which a is a primitive root mod p. For a non-square $a \in \mathbb{N}$, plot `ArtinCounts`(a, x) with increasing x (try this for different non-square a).