Computer Science & Engineering Department

IIT Kharagpur

Computational Number Theory: CS60094

Lecture X

Instructor: Goutam Biswas *Spring Semester 2014-2015*

1 Generators and Discrete Logarithm

We prove that for any prime p, $\mathbb{Z}_p^*$ is a cyclic group. We further show that for any odd prime p and any integer $e \geq 1$, $\mathbb{Z}_{p^e}^*$ is also a cyclic group. In case of $p = 2$, $\mathbb{Z}_2^* = \{1\}$ is a cyclic group. $\mathbb{Z}_{2^2}^* = \{1, 3\}$ also is a cyclic group. But $\mathbb{Z}_{2^3}^* = \{1, 3, 5, 7\}$ is not a cyclic group. It is known that $\mathbb{Z}_{2^e}$ for $e \geq 3$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2^{e-1}}$. But we shall not prove this result.

1.1 $\mathbb{Z}_p^*$ is cyclic for prime p

We prove a sequence of propositions to show that $\mathbb{Z}_p^*$ is a cyclic group for any odd prime p.
Definition 1: Given a group G, the smallest positive integer m, if it exists, is called the *exponent* of G if for all $g \in G$, $g^m = 1$.

Example 1. The exponent of $\mathbb{Z}_{15}^*$ is 4 as $1^4 = 2^4 = 4^4 = 7^4 = 8^4 = 11^4 = 13^4 = 14^4 = 1$. There is no other smaller integer satisfying this as $2^3 = 8$.
Proposition 1. Let G be a commutative group and $a, b \in G$ have orders m and n respectively, such that $gcd(m, n) = 1$. The order of ab is mn.

Proof: Let The order of ab be α. As $(ab)^{mn} = (a^m)^n(b^n)^m = 1 \cdot 1 = 1$, $\alpha | mn$. Again $1 = (ab)^{\alpha m} = (a^m)^\alpha b^{\alpha m} = 1 \cdot b^{\alpha m} = b^{\alpha m}$. So $n | \alpha m$, implies that $n | \alpha$. Similarly we can prove that $m | \alpha$. As m and n are coprimes, $mn | \alpha$. So $\alpha = mn$. QED.

Proposition 2. If the commutative group G has exponent m, then it contains an element of order m. A finite commutative group is cyclic if and only if its order is equal to its exponent.

Proof: Let $m = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorisation of m. Define $m_i = m/p_i$, $i = 1, \cdots, k$.
We claim that for each $i = 1, \cdots, k$, there is an $a_i \in G$ such that $a_i^{m_i} \neq 1$.
If that is not the case, then there is some i, $1 \leq i \leq k$, such that for all $a \in G$, $a^{m_i} = 1$. But that is impossible as m is the smallest such positive integer and $m_i < m$.

Let $a_1, \cdots, a_k \in G$ be such that $a_i^{m_i} \neq 1$, for each i, $1 \leq i \leq k$. Let $n_i = \frac{m}{p_i^{e_i}}$ and let $b_i = a_i^{n_i}$, for all $i = 1, \cdots, k$. We claim that the order of b_i is $p_i^{e_i}$, $i = 1, \cdots, k$.
We have $b_i^{p_i^{e_i - 1}} = (a_i^{n_i})^{p_i^{e_i - 1}} = a_i^{m/p_i} \neq 1$. But $b_i^{p_i^{e_i}} = (a_i^{n_i})^{p_i^{e_i}} = a_i^m = 1$.

The orders of b_i's are pairwise relatively prime. We have already proved that in a commutative group if the order of two elements a and b are coprime, them the order of ab is the product of their individual orders.
So the order of $\prod_{i=1}^k b_i$ is $p_i^{e_i} \cdots p_k^{e_k} = m$.

Let the size of G is m.
G is cyclic: there is an element $a \in G$ such that $< a >= G$. So the order of a is m and m is the exponent.
m is the exponent: there is an element whose order is m. So G is cyclic. QED.

Definition 2: Let R be a commutative ring with identity. An element $a \in R$ is called a *divisor* of an element $b \in R$ if there is a c such that $ac = b$. A *unit* of R is a divisor of the *identity* of R. The set of units of R is denoted by R^*.

If $a \in R$ is a *unit*, there is $b \in R$ such that $ab = 1$. If there is another $c \in R$ such that $ac = 1$, then

$$c = c \cdot 1 = c \cdot (ab) = (a \cdot c) \cdot b = 1 \cdot b = b.$$

We call b the inverse of a and denote it by a^{-1}.

Example 2. Two *units* of $\mathbb{Z}$ are ± 1. All non-zero elements are *units* of $\mathbb{Q}$.
Proposition 3. If R is a commutative ring with identity, then R^* is a commutative group under multiplication.

Proof: It is clear that $1 \in R^*$. If $a, b \in R^*$, then there are $c, d \in R$ such that $ac = 1 = bd$. So $(ab) \cdot (cd) = (ac) \cdot (bd) = 1 \cdot 1 = 1$. So R^* is closed under multiplication.
As $ac = 1$, we have $c = a^{-1} \in R^*$. QED.

If R is non-trivial and $R \setminus \{0\} = R^*$, then R is a *field* e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_p^*$ for any prime p are *fields*.
Definition 3: If R is a non-trivial commutative ring with identity and does not have any *zero divisor*, then it is an *integral domain*.
Proposition 4. If D is an *integral domain* and G is a finite subgroup of D^*, then G is cyclic.

Proof: Let the exponent of G be $m \leq |G|$. We know that for all $a \in G$, $a^m = 1$. So the elements of G are the roots of $X^m - 1 = 0$ in $D[X]$. But it is known that a polynomial of degree m over an integral domain has at most m roots. So $m = |G|$ and by the proposition (1.1) G is cyclic. QED.

Corollary 5. For every prime $\mathbb{Z}_p$ is a field and $\mathbb{Z}_p^*$ is finite and cyclic.

1.2 $\mathbb{Z}_{p^e}^*$ is Cyclic for Odd Prime p

We prove the following propositions.
Proposition 6. For every positive integer n and e, if $a \equiv b (\text{mod } n^e)$, then $a^n \equiv b^n (\text{mod } n^{e+1})$.

Proof: We have $a = b + kn^e$, so

$$a^n = (b + kn^e)^n = b^n + \binom{n}{1} b^{n-1} kn^e + \sum_{i=2}^{n} \binom{n}{i} b^{n-i} (kn^e)^i \equiv b^n (\text{mod } n^{e+1}).$$

QED.

Proposition 7. Let p be a prime and e be a positive integer such that $p^e > 2$. If $a \equiv 1 + p^e (\text{mod } p^{e+1})$, then $a^p \equiv 1 + p^{e+1} (\text{mod } p^{e+2})$.

Proof: Suppose $a \equiv 1 + p^e (\text{mod } p^{e+1})$. By the previous lemma (1.2), $a^p \equiv (1 + p^e)^p (\text{mod } p^{e+2})$. But then

$$(1 + p^e)^p = 1 + p \cdot p^e + \sum_{i=2}^{p-1} \binom{p}{i} p^{ei} + p^{ep}.$$

But we already know that $p | \binom{p}{i}$, when p is a prime and $0 < i < p$. So each term of the sum is divisible by p^{2e+1}. But then $e + 2 \leq 2e + 1$ for all $e \geq 1$. So each term of the sum is divisible by p^{e+2}. As $p^e > 2$, it is not possible that $p = 2$ and $e = 1$ i.e. $ep - e \geq 2$. So p^{ep} is divisible by p^{e+2}. QED.

Proposition 8. If p is an odd prime and e is a positive integer, then $\mathbb{Z}_{p^e}^*$ is cyclic.

Proof: We have already proved that $\mathbb{Z}_p^*$ is cyclic. So we take $e > 1$. Let $x \in \mathbb{Z}$ and $[x]_p$ generates $\mathbb{Z}_p^*$ i.e. the order of x is $p - 1$ ($x^{p-1} \equiv 1 (\text{mod } p)$. Let the *multiplicative order* of x in $\mathbb{Z}_{p^e}^*$ be m i.e. $x^m \equiv 1 (\text{mod } p^e)$. So we have $x^m \equiv 1 (\text{mod } p)$. This implies that $(p - 1)$ divides m and we conclude that $(x^{m/p-1})^{p-1} = x^m \equiv 1 (\text{mod } p^e)$ i.e. the multiplicative order of $x^{m/p-1}$ in $\mathbb{Z}_{p^e}$ is $p - 1$. If we can find an y so that the multiplicative order of y in $\mathbb{Z}_{p^e}^*$ is p^{e-1}, then we have the element $x^{m/p-1} \cdot y$ whose order is $p^{e-1}(p - 1)$ in $\mathbb{Z}_{p^e}^*$.

We take $y = 1 + p$. All elements of $\mathbb{Z}_{p^e}$ can be encoded as a e-digit number in *radix-p*. The representation for y is $0 \cdots 011 = p^1 + p^0$.
According to propositon (1.2), $y = 1 + p$ implies $y^p \equiv 1 + p^2 (\text{mod } p^3)$. So the value of y^p mod p^3 is "101" in *radix-p* numeral. Clearly these three digits remain the same for e-digit representation of y^p mod p^e. In the same way we have the following values:

$$\begin{array}{rcl} y \bmod p^e & = & \overbrace{0 \cdots 011}^{e} \\ y^p \bmod p^e & = & \overbrace{a_{e-1} \cdots a_3 101}^{e},\ y^p \equiv 1 + p^2 (\text{mod } p^3) \\ y^{p^2} \bmod p^e & = & \overbrace{b_{e-1} \cdots b_3 1001}^{e},\ y^{p^3} \equiv 1 + p^3 (\text{mod } p^4) \\ \vdots & \vdots & \vdots \\ y^{p^{e-2}} \bmod p^e & = & \overbrace{10 \cdots 001}^{e},\ y^{p^{e-2}} \equiv 1 + p^{e-1} (\text{mod } p^e) \\ y^{p^{e-1}} \bmod p^e & = & \overbrace{00 \cdots 001}^{e},\ y^{p^{e-1}} \equiv 1 + p^e (\text{mod } p^e) \end{array}$$

So the order of y is p^{e-1}. QED.

Example 3. We know that $\mathbb{Z}_5^*$ is a cyclic group with generator 2. The generator for $\mathbb{Z}_{5^2}$ is $2 \times (5 + 1) = 12$. Note that the multiplicative order of 2 in $\mathbb{Z}_{5^2}$ is 4 $(2, 4, 3, 1)$ and that of 6 is 5 $(6, 11, 16, 21, 1)$. As the $gcd(4, 5) = 1$, the multiplicative order of $6 \times 2 = 12$ in $\mathbb{Z}_{5^2}$ is $5 \times 4 = \phi(25)$. So 12 is a generator of $\mathbb{Z}_{5^2}$.

1.3 Generator and Discrete Log in $\mathbb{Z}_p^*$

We know that for any prime p, $\mathbb{Z}_p^*$ is a *cyclic group*. So there are $\phi(p-1)$ generators of $\mathbb{Z}_p^*$. If g is a generator of $\mathbb{Z}_p^*$ and $y \in \mathbb{Z}_p^*$, then there is an integer x, $0 \leq x < p-1$ such that $g^x = y$. The integer x is called the *discrete logarithm* of y to the base g in $\mathbb{Z}_p^*$, $\log_g y = x$.

So we have two important computational problems - finding a generator g of $\mathbb{Z}_p^*$ and given a g and y, finding the *discrete log* x. If $g \in G$ is not a generator, but generates a subgroup G of $\mathbb{Z}_p^*$, such that the order of $< g >= G$ is q. We know that $q | p-1$. In this case if $y \in G$, then $g^x = y$ or $\log_g y = x$, where $0 \leq x < q$.

1.3.1 Generator for $\mathbb{Z}_p^*$

There is no known efficient algorithm for finding generator of $\mathbb{Z}_p^*$. Even if the prime factorisation of $p-1$ is given, we have probabilistic algorithm. The input to the algorithm is an odd prime p and the prime factorisation of $p-1$. The output is a generator of $\mathbb{Z}_p^*$. Let

$$p - 1 = \prod_{i=1}^{k} p_i^{e_i}.$$

Our algorithm relies on the following proposition.
Proposition 9. G is a commutative group and $a \in G$ is such that for some prime p and an integer $e \geq 1$, $a^{p^e} = 1$, but $a^{p^{e-1}} \neq 1$, then the order of a is p^e.

Proof: Let m be the order of a. So $m | p^e$ i.e. $m = p^f$, $0 \leq f \leq e$. If $f < e$, then $a^{p^{e-1}} = (a^{p^f})^{p^{e-f-1}} = 1^{p^{e-f-1}} = 1$ - is a contradiction. QED.

In the randomised algorithm we pick up (at random) $a_1, \cdots, a_k$ so that the order of $g_i = a_i^{(p-1)/p_i}$, is $p_i^{e_i}$, for $i = 1, \cdots, k$. It is known that the order of $\prod_{i=1}^{k} g_i$ is $\prod_{i=1}^{k} p_i^{e_i} = p - 1$.

```
for i ← 1 to k
    repeat
        a ← rand{1, ··· p − 1}
        b ← a^{(p−1)/p_i}
    until b ≠ 1
    g_i ← a^{(p−1)/p_i^{e_i}}
g ← ∏_{i=1}^{k} g_i
return g
```

We establish the correctness of the algorithm. Let $q_i = (p-1)/p_i^{e_i}$. So $1 \neq b = (a^{q_i})^{p_i^{e_i-1}} = g_i^{p_i^{e_i-1}}$, but $g_i^{p_i^{e_i}} = a^{p-1} = 1$. So the order of g_i is $p_i^{e_i}$. As $gcd(p_i^{e_i}, p_j^{e_j}) = 1$, $1 \leq i < j \leq k$, the order of g is $p-1$. The algorithm if terminates gives correct output.

References

[VS] *A Computational Introduction to Number Theory and Algebra* by Victor Shoup, 2nd ed., Pub. Cambridge University Press, 2009, ISBN 978-0-521-51644-0.