The structure of $\mathbb{Z}_n^*$

Mathematical Cryptography,
Lectures 11 - 12

Contents

Group exponent

By Euler's theorem, $a^{|G|} = 1$ for every element $a \in G$. However, $|G|$ need not be the smallest exponent to which we must power even any element $a \in G$ to get the identity 1.

Definition

Let $(G, \cdot)$ be a group with the identity element 1. The smallest positive integer $m > 0$, such that for every $a \in G$ is $a^m = 1$, is called the *exponent of the group* G. We denote it by $\exp(G)$. If no such m exists, we set $\exp(G) = 0$.

Examples

- $\exp(\mathbb{Z}_n) = n$, $\exp(\mathbb{Z}) = 0$
- $\exp(\mathbb{Z}_9^*) = 6 = \varphi(9)$
- $\exp(\mathbb{Z}_8^*) = 2 < \varphi(8)$

Group exponent

Proposition

- If G is a finite group, then G has a positive exponent and $\exp(G) \mid |G|$.
- If the group G has a positive exponent, then every element $a \in G$ has a finite order and $\mathrm{r}(a) \mid \exp(G)$.
- If the group G is cyclic, then $\exp(G) = 0$ iff G is infinite, and $\exp(G) = |G|$ iff G is finite.
- If G_1, G_2 are groups, then $\exp(G_1 \times G_2) = \mathrm{lcm}(\exp(G_1), \exp(G_2))$.

Group exponent

Proposition

If an abelian group G has a positive exponent $\exp(G) = m > 0$, then it contains an element of order m.

Proof: Let $m = \prod_{i=1}^{k} p_i^{e_i}$.
For any $1 \leq i \leq k$ we can find an element $b_i \in G$ such that $b_i^{\frac{m}{p_i}} \neq 1$, otherwise $\exp(G) \leq \frac{m}{p_i} < m$.
Let $m_i = \frac{m}{(p_i^{e_i})}$, then $a_i = b_i^{m_i}$ has an order $\mathrm{r}(a_i) = p_i^{e_i}$.
Set $a = \prod_{i=1}^{k} a_i$, then an order $\mathrm{r}(a) = m$ due to the pairwise relatively primeness of the orders $\mathrm{r}(a_i)$.

Consequence

A finite abelian group G is cyclic if and only if $\exp(G) = |G|$.

The structure of $\mathbb{Z}_n^*$

For which $n \in \mathbb{N}$ is the group $\mathbb{Z}_n^*$ cyclic?
First we show that groups $\mathbb{Z}_p^*$, where p is a prime, are cyclic, using the fact that $(\mathbb{Z}_p, +, \cdot)$ is a field.

Proposition

A non-zero polynomial of the degree m over a field has at most m distinct roots.

Note

The proposition is true for polynomials over an integrity domain (a ring with no zero divisors) too, but not over any ring.
For example, $x^2 - 1$ has four roots in $\mathbb{Z}_8$, namely $\pm 1, \pm 3$.

The structure of $\mathbb{Z}_n^*$

Proposition

The group $\mathbb{Z}_p^*$ is cyclic for each prime p.

Proof: Denote $\exp(\mathbb{Z}_p^*) = m \leq p - 1$.
Any element $a \in \mathbb{Z}_p^*$ satisfies $a^m = 1$, so it is a root of $x^m - 1$.
Since $\mathbb{Z}_p$ is a field, $m = p - 1$ must hold.
The element of order $\exp(\mathbb{Z}_p^*) = p - 1$ (which exists) is the generator of $\mathbb{Z}_p^*$.

Proposition

The group T^* is cyclic for every finite field T (or for every finite integrity domain).

The structure of $\mathbb{Z}_n^*$

Next we examine groups $\mathbb{Z}_{p^e}^*$, where p is a prime.

Proposition

Let p be a prime. For every $1 \leq k \leq p-1$ is $p \mid \binom{p}{k}$

Lemma 1

Let p be a prime and $e \geq 1$ be a natural number.
If $a \equiv b (\mod p^e)$ then $a^p \equiv b^p (\mod p^{e+1})$.

Lemma 2

Let p be a prime and $e \geq 1$ be a natural number and let $p^e > 2$.
If $a \equiv 1 + p^e (\mod p^{e+1})$ then $a^p \equiv 1 + p^{e+1} (\mod p^{e+2})$.

The structure of $\mathbb{Z}_n^*$

Proposition

The group $\mathbb{Z}_{p^e}^*$ is cyclic for every odd prime p (i.e. $p > 2$) and every natural number $e \geq 2$.

Thus $\exp(\mathbb{Z}_{p^e}^*) = |\mathbb{Z}_{p^e}^*| = p^{e-1}(p-1)$.

Proof: Let a be a generator of the group $\mathbb{Z}_p^*$ and let r denote the order of a in the group $\mathbb{Z}_{p^e}^*$. Then $b = a^{\frac{r}{p-1}}$ has order $p-1$ in $\mathbb{Z}_{p^e}^*$. It can be shown that $c = 1 + p$ has order p^{e-1} in $\mathbb{Z}_{p^e}^*$ by lemma 2. Since $\gcd(p^{e-1}, p-1) = 1$, then $\mathrm{r}(bc) = p^{e-1}(p-1)$. So the element bc is a generator of $\mathbb{Z}_{p^e}^*$.

The structure of $\mathbb{Z}_n^*$

Proposition

The groups $\mathbb{Z}_2^*$ and $\mathbb{Z}_4^*$ are cyclic.
The group $Z_{2^e}^*$ is not cyclic for every natural number $e \geq 3$.
Thus $\exp(\mathbb{Z}_{2^e}^*) = \frac{|\mathbb{Z}_{2^e}^*|}{2} = 2^{e-2}$.

Proof: It can proved that $c = 5$ has order 2^{e-2} by lemma 2.
Moreover, $-1 \notin \langle 5 \rangle$. Hence, $\mathbb{Z}_{2^e}^*$ is an internal direct product
$\mathbb{Z}_{2^e}^* = \langle -1 \rangle \dot{\times} \langle 5 \rangle$.
$\exp(\mathbb{Z}_{2^e}^*) = \mathrm{lcm}(2, 2^{e-2}) = 2^{e-2}$ and $\mathbb{Z}_{2^e}^*$ is not cyclic.

The structure of $\mathbb{Z}_n^*$

Finaly we study groups $\mathbb{Z}_n^*$ where n is divisible by at least two distinct primes.

Proposition

The group $\mathbb{Z}_{2p^e}^*$ is cyclic for every odd prime $p > 2$ and every natural number $e \geq 1$.

Proposition

The group $\mathbb{Z}_n^*$ is not cyclic for every composite number $n = n_1 n_2$, where $2 < n_1 < n_2$ and $\gcd(n_1, n_2) = 1$.

In this case, $\exp(\mathbb{Z}_n^*) = \operatorname{lcm}(\exp(\mathbb{Z}_{n_1}^*), \exp(\mathbb{Z}_{n_2}^*)) \leq \frac{|\mathbb{Z}_n^*|}{2}$.

Proof: Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$, then from the Chinese remainder theorem, $\mathbb{Z}_n^* \cong \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$.

The structure of $\mathbb{Z}_n^*$

Summary

The group $\mathbb{Z}_n^*$ is cyclic just when

$$n = 1, 2, 4, p^e, 2p^e,$$

where p is an odd prime and e is a positive integer.

Carmichael's function

Definition

The function $\lambda : \mathbb{N}^+ \to \mathbb{N}^+ : \lambda(n) = \exp(\mathbb{Z}_n^*)$ is called the *Carmichael's function*. Or $\lambda(n)$ for $n > 1$ is the smallest $m > 0$ such that for all a relatively prime to n is $a^m = 1$ in $\mathbb{Z}_n$. Furthermore, $\lambda(1) = 1$.

Formulas

- $\lambda(p^e) = p^{e-1}(p-1) = \varphi(p^e)$ for primes $p > 2$
- $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^e) = 2^{e-2} = \frac{\varphi(2^e)}{2}$ for $e \geq 3$
- $\lambda(n_1 \cdot n_2) = \mathrm{lcm}(\lambda(n_1), \lambda(n_2))$ for n_1, n_2 relatively prime

Carmichael's function

Note

RSA-encryption will work even if the keys are inverses to aech other modulo $\lambda(n)$, or modulo an integer multiple $k\lambda(n)$, where $k > 0$.

Corollary: If we use Carmichael's numbers instead of primes p, q when creating the key protocol, the RSA-encryption will work.

A *Carmichael's number* is a composite number n such that for every $a \in \mathbb{Z}_n^*$ is $a^{n-1} = 1$ in $\mathbb{Z}_n$.
For a Carmichael's number n is $\lambda(n) \mid n - 1$.

The Fermat's primality test does not distinguish Carmichael's numbers from primes.

Equations $x^m = 1$ in $\mathbb{Z}_n$

Residual isomorphism

Let $n = \prod_{i=1}^{k} p_i^{e_i}$, where primes p_i are different.
The map $\theta : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{e_1}} \times \ldots \times \mathbb{Z}_{p_k^{e_k}} : a \mapsto (a_1, \ldots, a_k)$, where each $0 \leq a_i < p_i^{e_i}$ satisfies $a \equiv a_i \pmod{p_i^{e_i}}$, is a ring isomorphism (the Chinese residual isomorphism): $\mathbb{Z}_n \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i}}$
The restriction of θ to the set $\mathbb{Z}_n^*$ is a group isomorphism of multiplicative groups: $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \ldots \times \mathbb{Z}_{p_k^{e_k}}^*$

Consequence

An equation $x^m = 1$ can be solved residually, since $a^m = 1$ in $\mathbb{Z}_n$ if and only if $a_i^m = 1$ in $\mathbb{Z}_{p_i^{e_i}}$ for every $1 \leq i \leq k$.

Equations $x^m = 1$ in $\mathbb{Z}_n$

Proposition

If $a \in \mathbb{Z}_n$ solves $x^m = 1$, then a is invertible, so $a \in \mathbb{Z}_n^*$.

So, we have to solve $x^m = 1$ in the group $Z_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \ldots \times \mathbb{Z}_{p_k^{e_k}}^*$.

- In cyclic groups $\mathbb{Z}_{p_i^{e_i}}^*$, where $p_i > 2$, we can find all solutions of $x^m = 1$ using the generator. The number of solutions is $d_i = \gcd(m, \varphi(p_i^{e_i}))$.
- In the group $\mathbb{Z}_{2^e}^*$ we find all solutions of $x^m = 1$ in the cyclic subgroup $\langle 5 \rangle$ of order 2^{e-2}, there is $\gcd(m, 2^{e-2})$ solutions. That is all for m odd, but for m even, we should add the opposite solutions (of the form $-a$, where a is a solution).
- In $\mathbb{Z}_n^*$ is $d = \prod_{i=1}^k d_i$ solutions altogether, they are of the form $a = a_1 q_1 + \cdots + a_k q_k$, where q_i are from the Chinese remainder theorem.

Equations $x^m = 1$ in $\mathbb{Z}_n$

Example

Solve $x^6 = 1$ in $\mathbb{Z}_{304}$.

Each solution lies in $\mathbb{Z}_{304}^* \cong \mathbb{Z}_{19}^* \times \mathbb{Z}_{16}^*$.

- $\mathbb{Z}_{19}^* = \langle 2 \rangle$, $\varphi(19) = 18$. The equation here has 6 solutions, namely $x \in \langle 2^3 \rangle = \{\pm 1, \pm 7, \pm 8\}$.
- $\mathbb{Z}_{16}^* = \langle 5 \rangle \times \langle -1 \rangle$, in the subgroup $\langle 5 \rangle$ the equation reduces to $x^2 = 1$ and is solved by $x \in \langle 5^2 \rangle = \{9, 1\}$. The exponent is even, so all solutions are $x \in \{\pm 1, \pm 9\}$.

In $\mathbb{Z}_{304}^*$ there is $6 \cdot 4 = 24$ solutions of the form $x \in \{\pm 1, \pm 7, \pm 8\} q_{19} + \{\pm 1, \pm 9\} q_{16}$, where $q_{19} = 96$, $q_{16} = -95$ are obtained by solving the diophantine equation $16t + 19r = 1$.

Equations $x^m = 1$ in $\mathbb{Z}_n$

Squares and square roots in $\mathbb{Z}_n^*$

- Let p be an odd prime, then the equation $x^2 = 1$ has just two solutions in $\mathbb{Z}_{p^e}^*$, namely $x = \pm 1$.
  The group homomorphism $\rho_2 : \mathbb{Z}_{p^e}^* \to \mathbb{Z}_{p^e}^* : a \mapsto a^2$ has $|Ker\,\rho_2| = 2$, $|Im\,\rho_2| = \frac{\varphi(p^e)}{2}$.
- Let $n = \prod_{i=1}^k p_i^{e_i}$ be an odd number, then $x^2 = 1$ has together 2^k solutions in $\mathbb{Z}_n^*$.
  The group homomorphism $\rho_2 : \mathbb{Z}_n^* \to \mathbb{Z}_n^* : a \mapsto a^2$ has $|Ker\,\rho_2| = 2^k$, $|Im\,\rho_2| = \frac{\varphi(n)}{2^k}$.

Equations $x^m = x$ in $\mathbb{Z}_n$

Observation

If $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$, then the equation $x^m = x$ can have non-zero non-invertible solutions in the monoid $\mathbb{Z}_n$. For example, $a \in \mathbb{Z}_n$, where $\theta(a) = (0, 1)$, is a nonzero solution not relatively prime to n_1.
In $\mathbb{Z}_n$ the equation cannot be canceled by x (even assuming $x \neq 0$), and it is not sufficient to solve $x^m = x$ in the group $\mathbb{Z}_n^*$.

Proposition

The element a solves the equation $x^m = x$ in $\mathbb{Z}_{p^e}$ if and only if either $a = 0$ or a solves the equation $x^{m-1} = 1$ in $\mathbb{Z}_{p^e}$.

We are able to solve $x^m = x$ in $\mathbb{Z}_n$ residually. For example, we can compute all messages which do not change by RSA encryption.

Equations $x^m = b$ in $\mathbb{Z}_n$

Note

All solutions of the equation $x^m = b$ in $\mathbb{Z}_n$ are of the form $x = ac$, where a is one particular solution of this equation, and c is any solution of the equation $x^m = 1$ in $\mathbb{Z}_n$.

We did not give instructions for finding a particular $m-$th root of b, we only gave the procedure for finding all $m-$th roots of 1, which relied on the fact that we know the factorization of n.

It is believed that counting the $m-$th roots in $\mathbb{Z}_n$ without knowing the factorization of n is an exponentially hard problem (by brute force). This is the cause of the security of the RSA encryption.

The structure of $\mathbb{Z}_n^*$

Literature

- Shoup: A Computational Introduction to Number Theory and Algebra. Chapters 6.5 and 7.5.
  http://shoup.net/ntb/