Chapter 4: The Structure of $U(\mathbb{Z}/n\mathbb{Z})$

Theorem 1. *$U(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group.*

Proof. Let $p-1 = q_1^{e_1} q_2^{e_2} \cdots q_t^{e^t} = \prod_q q^e$ be the prime decomposition of $p-1$. Consider the congruences

(1) $x^{q^{e-1}} \equiv 1(p)$

(2) $x^{q^e} \equiv 1(p)$

Therefore,

(1) Every solution to $x^{q^{e-1}} \equiv 1\,(p)$ is a solution of $x^{q^e} \equiv 1\,(p)$.

(2) $x^{q^e} \equiv 1\,(p)$ has more solutions than $x^{q^{e-1}} \equiv 1\,(p)$. In fact, $x^{q^{e-1}} \equiv 1\,(p)$ has q^{e-1} solutions and $x^{q^e} \equiv 1\,(p)$ has q^e solutions by Proposition 4.1.2.

Therefore, there exists $g_i \in \mathbb{Z}/p\mathbb{Z}$ generating a subgroup of $U(\mathbb{Z}/p\mathbb{Z})$ of order $q_i^{e_i}$ for all $i = 1, ..., t$. Pick $g = g_1 g_2 \cdots g_t \in \mathbb{Z}/p\mathbb{Z}$ generating a subgroup of $U(\mathbb{Z}/p\mathbb{Z})$ of order $q_1^{e_1} q_2^{e_2} \cdots q_t^{e^t} = p-1$. That is, $\langle g \rangle = U(\mathbb{Z}/p\mathbb{Z})$. $\square$

Exercise 4.1. *Show that 2 is a primitive root module 29.*

Proof. $2^1 \equiv 2\,(29)$, $2^2 \equiv 4\,(29)$, $2^3 \equiv 8\,(29)$, $2^4 \equiv 16\,(29)$, $2^5 \equiv 3\,(29)$, $2^6 \equiv 6\,(29)$, $2^7 \equiv 12\,(29)$, $2^8 \equiv 24\,(29)$, $2^9 \equiv 19\,(29)$, $2^{10} \equiv 9\,(29)$, $2^{11} \equiv 18\,(29)$, $2^{12} \equiv 7\,(29)$, $2^{13} \equiv 14\,(29)$, $2^{14} \equiv 28\,(29)$, $2^{15} \equiv 27\,(29)$, $2^{16} \equiv 25\,(29)$, $2^{17} \equiv 21\,(29)$, $2^{18} \equiv 13\,(29)$, $2^{19} \equiv 26\,(29)$, $2^{20} \equiv 23\,(29)$, $2^{21} \equiv 17\,(29)$, $2^{22} \equiv 5\,(29)$, $2^{23} \equiv 10\,(29)$, $2^{24} \equiv 20\,(29)$, $2^{25} \equiv 11\,(29)$, $2^{26} \equiv 22\,(29)$, $2^{27} \equiv 15\,(29)$, $2^{28} \equiv 1(29)$. Thus $U(\mathbb{Z}/29\mathbb{Z}) = \langle 2 \rangle$. $\square$

Exercise 4.11. *Prove that $1^k + 2^k + \cdots + (p-1)^k \equiv 0\,(p)$ if $p-1 \nmid k$ and $-1(p)$ if $p-1 \mid k$.*

Proof. Write $\langle g \rangle = U(\mathbb{Z}/p\mathbb{Z})$, and $S = 1^k + 2^k + \cdots + (p-1)^k \equiv g^k + (g^k)^2 + \cdots + (g^k)^{p-1}\,(p)$.

If $p-1 \mid k$, $g^k \equiv 1\,(p)$. Thus $S \equiv 1 + 1 + \cdots + 1 = p-1 \equiv -1\,(p)$.

If $p-1 \nmid k$, g^k is also a generator of $U(\mathbb{Z}/p\mathbb{Z})$ by Exercise 13. There are three proofs of this case.

(1) S is the sum of a geometric series. So $(1-g^k)S = g^k(1-(g^k)^{p-1}) = g^k(1-(g^{p-1})^k) \equiv 0\,(p)$. Since $g^k \not\equiv 1\,(p)$, $S \equiv 0\,(p)$.

(2) $\langle g^k \rangle = U(\mathbb{Z}/p\mathbb{Z})$. So $S \equiv g^k + (g^k)^2 + \cdots + (g^k)^{p-1} \equiv 1 + 2 + \cdots + (p-1) \equiv \frac{p(p-1)}{2} \equiv 0\,(p)$ since p is odd and thus $\frac{p-1}{2}$ is an integer. (If $p = 2$ is even, then there does not exist any k such that $p-1 \nmid k$.)

(3) Similar to (2), write $S \equiv 1+2+\cdots+(p-1)\,(p)$. Notice that the equation $x^{p-1}-1 \equiv (x-1)(x-2)\cdots(x-(p-1))\,(p)$ holds by Proposition 4.1.1. So $S \equiv 0\,(p)$ by comparing the coefficient of x^{p-2} on the both sides if $p > 2$. (Again $p = 2$ is impossible in this case.)

$\square$

Exercise 4.12. *Use the existence of a primitive root to give another proof of Wilson's theorem* $(p-1)! \equiv -1\,(p)$.

Proof. Say $p > 2$. ($p = 2$ is trivial.) Let g be a primitive root of $U(\mathbb{Z}/p\mathbb{Z})$. So $(p-1)! \equiv g \cdot g^2 \cdots g^{p-1} \equiv g^{\frac{p(p-1)}{2}}\,(p)$.

The equation $x^2 \equiv 1\,(p)$ has exactly 2 solutions $x \equiv 1, -1\,(p)$ by Proposition 4.1.2. Notice that $x \equiv g^{\frac{p-1}{2}}\,(p)$ is a solution of the equation $x^2 \equiv 1\,(p)$ and $g^{\frac{p-1}{2}} \not\equiv 1\,(p)$ since g is a primitive root of $U(\mathbb{Z}/p\mathbb{Z})$. Therefore,

$$g^{\frac{p-1}{2}} \equiv -1\,(p).$$

So $(p-1)! \equiv g^{\frac{p(p-1)}{2}} \equiv (-1)^p \equiv -1\,(p)$ since p is an odd prime. $\square$

Supplement 1. There are many proofs of Wilson's theorem.

(1) Exercise 3.9. Use a reduced residue system modulo p.

(2) Corollary of Proposition 4.1.1. $x^{p-1}-1 \equiv (x-1)(x-2)\cdots(x-p+1)\,(p)$.

(3) Exercise 4.12. Use the existence of a primitive root.

(4) Inclusion-exclusion principle (Enrique Trevio, An Inclusion-Exclusion Proof of Wilson's Theorem).
Lemma.

$$n! = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^n.$$

Proof of lemma. Consider the number of permutations on $S = \{1, 2, ..., n\}$. On the one hand, the number is $n!$. On the other hand, we can think of a permutation on S as a function $f : S \to S$ that is onto. The number of functions $g : S \to S$ is n^n. To find the onto functions, we have to remove whichever ones are not onto. Therefore, we must remove those that miss at least 1 value. There are $\binom{n}{1}$ ways of choosing the missed value and $(n-1)^n$ functions missing that particular value. But when we remove all of these functions, we took out some too many times, indeed, any function that misses at least 2 values was over counted. So we have to add it back in. We get $\binom{n}{2}(n-2)^n$ such functions. Continue this process. $\square$

Proof. Now we use the equation $n! = \sum_{k=0}^{n}(-1)^k\binom{n}{k}(n-k)^n$ by substituting $n = p-1$ and then get

$$(p-1)! = \sum_{k=0}^{p-1}(-1)^k\binom{p-1}{k}(p-1-k)^{p-1}.$$

Now look at the k-term in the summation.

$k!(p-1-k)! \equiv (-1)^k(p-k)(p-(k-1))\cdots(p-1)\cdot(p-1-k)! \equiv (-1)^k(p-1)!\ (p)$. So $\binom{p-1}{k} = \frac{(p-1)!}{k!(p-1-k)!} \equiv (-1)^k\ (p)$. Also, $(p-1-k)^{p-1} \equiv (-1-k)^{p-1} \equiv (1+k)^{p-1}\ (p)$ since $(-1)^{p-1} = 1$ if $p > 2$. ($p = 2$ is trivial.) Therefore,

$$(p-1)! \equiv \sum_{k=0}^{p-1}(-1)^k\cdot(-1)^k\cdot(1+k)^{p-1} \equiv \sum_{k=1}^{p-1}k^{p-1}\ (p).$$

(We adjust the index of the summation and notice that $p^{p-1} \equiv 0\ (p)$). By Fermats Little Theorem, $k^{p-1} \equiv 1\ (p)$. Therefore, the right-hand sum consists of $(p-1)$ ones and the proof is completed. □

The original proof in the paper is not very beautiful. We don't need to use the inclusion-exclusion expression of $p!$ and then cancel out p on the both sides. Please use $(p-1)!$ directly.

(5) One combinatorial proof (Cheenta, Wilson's Theorem and It's Geometric proof).
Proof. Consider a circumference with p points that correspond to the vertices of a regular p-gon. There are $\frac{(p-1)!}{2}$ (non-regular or regular) polygons that we form by joining these vertices.

Now among $\frac{(p-1)!}{2}$ of them, we have $\frac{p-1}{2}$ unaltered when rotated by $\frac{2\pi}{p}$ radian. That is, there are $\frac{p-1}{2}$ regular polygons due to the rotational symmetry.

Therefore, there are $\frac{(p-1)!}{2} - \frac{p-1}{2}$ non-regular polygons. Notices that the number of non-regular polygons is divided by p since p is a prime.

So $\frac{(p-1)!}{2} - \frac{p-1}{2} \equiv 0\ (p)$. Hence, $(p-1)! \equiv p-1 \equiv -1\ (p)$ if $p > 2$. ($p = 2$ is trivial.) □

Supplement 2. Related problems.

(1) (ProjectEuler 381: (prime-k) factorial). *Let* $S(p) = \sum_{1\le k\le 5}(p-k)!\ (p)$ *for a prime* p. *Find* $\sum_{1\le p\le 10^8} S(p)$ (by using computer programs).

(2) *Let g be a primitive root modulo the odd prime p. Prove that $g^{\frac{p-1}{2}} \equiv -1(p)$. Deduce that if g, h are primitive roots modulo the odd prime p then $g \cdot h$ cannot be a primitive root.*

Exercise 4.13 (Generators of a cyclic group). *Let G be a finite cyclic group and $g \in G$ is a generator. Show that all the other generators are of the form g^k, where $(k, n) = 1$, n being the order of G.*

Proof. Suppose that $h = g^k$ with $(k, n) = 1$. Then clearly $\langle h \rangle \subseteq \langle g \rangle$ as a subset. For the reverse containment ($\supseteq$), write $rk + sn = 1$ where $r, s \in \mathbb{Z}$. Then $h^r = g^{kr} = g^{1-sn} = g \cdot (g^n)^{-s} = g \cdot 1 = g$. Then again $\langle g \rangle \subseteq \langle h \rangle$ as a subset.

Now suppose that $\langle g \rangle = \langle h \rangle$. Then $h = g^k$ for some $k \in \mathbb{Z}$. Also, $g = h^r$ for some $r \in \mathbb{Z}$. So $g = h^r = g^{kr}$ or $g^{kr-1} = 1$. So $n|(kr - 1)$, or $ar + ns = 1$ for some $s \in \mathbb{Z}$, that is, $(a, n) = 1$. $\square$

Reference: R. C. Daileda, The Structure of $U(\mathbb{Z}/n\mathbb{Z})$.

Corollary. *Let G be a finite cyclic group of order n. Then G has exactly $\phi(n)$ generators.*

Corollary. *$U(\mathbb{Z}/p\mathbb{Z})$ has exactly $\phi(p-1)$ generators. $U(\mathbb{Z}/p^l\mathbb{Z})$ has exactly $\phi(p^{l-1}(p-1))$ generators if p is odd.*