Math 342 Tutorial
July 2, 2025

Recall a group G is cyclic if there is some $g \in G$ for which $G = \{g^n : n \in \mathbf{Z}\}$. If G is finite with n distinct elements, then $G = \{1, g, g^2, \ldots, g^{n-1}\}$. We often use the notation $G = \langle g \rangle$ in this case.

Question 1. Let $G = \langle g \rangle$ be a finite cyclic group of order n. Show that for every divisor d of n, there is a unique subgroup H of G of order d. Show, moreover, that H is cyclic.

Let d be a nontrivial divisor of n, and let $h = g^{n/d}$. Certainly, $h^d = g^n = 1$, hence $\mathrm{ord}(h) \mid d$. Suppose there is a nontrivial divisor d_1 of d for which $h^{d_1} = 1$. Then $g^{nd_1/d} = 1$, but $nd_1/d < n$ which contradicts the fact that $\mathrm{ord}(g) = n$.

We have shown that G has a cyclic group of order d for every nontrivial divisor d of n. Conversely, suppose that H is a (not necessarily cyclic) subgroup of G of order d. By the Well-Ording Principal, there is a positive integer m for which m is the smallest exponent of a power of g appearing in H. For an integer k, and by the Division Algorithm, there are uniquely determined integers q and r with $0 \leqq r < m$ for which $k = qm + r$. Suppose $g^k = g^{qm+r} \in H$; then $g^r \in H$ since $g^{qm} \in H$. By the minimality of m, we have that $r = 0$. It follows that every element of H is of the form g^{qm} for some integer q. We have shown that $H \subseteqq \langle g^m \rangle$. As $g^m \in H$, we have also that $\langle g^m \rangle \subseteqq H$. We have shown therefore that H is cyclic.

Question 2. Fill in the details of the following argument to show that $(\mathbf{Z}/p\mathbf{Z})^*$, the nonzero residues modulo p, form a cyclic group.

(a) Let $h = q_1^{r_1} \cdots q_s^{r_s}$ be the prime power factorization of $h = p - 1$. Show that for every $1 \leqq i \leqq s$, there is a nonzero residue which is not a root of $x^{h/p_i} - 1$ modulo p.

(b) Let a_i be a nonzero residue which is not a root of $x^{h/p_i} - 1$, and define $b_i = a_i^{h/p_i^{r_i}}$. Show that $\mathrm{ord}_p(b_i) = p_i^{r_i}$.

(c) Show the element $b = b_1 \cdots b_s$ has multiplicative order $h = p - 1$. In particular, this shows that $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclic. We call b a primitive root modulo p.

By a result of Lagrange, there are at most $h/p_i < h$ roots of $x^{h/p_i} - 1$ modulo p. Therefore, there is a nonzero residue a_i which is not such a root. Defining $b_i = a_i^{h/p_i^{r_i}}$, we see that $b_i^{p_i^{r_i}} = a_i^h = 1$ whereupon $\mathrm{ord}(b_i) \mid p_i^{r_i}$. But $b_i^{p_i^{r_i - 1}} = a^{h/p_i} \neq 1$, hence $\mathrm{ord}(b_i) = p_i^{r_i}$.

Define $b = b_1 \cdots b_s$, and suppose that $\mathrm{ord}(b)$ is a proper divisor of $h = p - 1$. Therefore, $\mathrm{ord}(b)$ divides one of the s integers h/p_i, say h/p_1. For $i > 1$, we have that $b_i^{h/p_1} = 1$ (why?). It follows that $b^{h/p_1} = b_1^{h/p_1} = 1$. Therefore, $\mathrm{ord}(b_1) \mid h/p_1$; but this is impossible since we have already shown that $\mathrm{ord}(b_1) = p_1^{r_1}$.

Compare the previous question with Question 6 of the previous tutorial set.

Question 3. Use Questions 1 and 2 to show the following. **(a)** $a^p \equiv a \pmod{p}$ for every integer a. **(b)** $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

(a) We have already shown that $(\mathbf{Z}/p\mathbf{Z})^*$ is a cyclic group of order $p - 1$. Let $g \in (\mathbf{Z}/p\mathbf{Z})^*$ be such that $(\mathbf{Z}/p\mathbf{Z})^* = \langle g \rangle$. For every nonzero residue g^k, we have shown that $\langle g^k \rangle$ is a subgroup of order $(p - 1)/(k, n)$. Thus, $(g^k)^{p-1} = (g^{[p-1, k]})^{(p-1, k)} = 1^{(p-1, k)} = 1$. It follows that $a^p \equiv a \pmod{p}$ whenever p does not divide a. If $p \mid a$, then $a \equiv 0 \pmod{p}$ and the result is trivial.

(b) From what we have shown, the quadratic residues are the subgroup $\langle g^2 \rangle$ which are exactly those nonzero residues a for which $a^{(p-1)/2} = 1$. Since $\operatorname{ord}(a^{(p-1)/2}) \leqq 2$, if $a^{(p-1)/2} \neq 1$, i.e., it is not a quadratic residue, then $a^{(p-1)/2} = -1$.

Question 4. We will give a second proof of the fact that $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. Fill in the following details.

(a) Let i be the principal root of -1. Show that $(1+i)^2 = 2i$. Use this to show that $(1+i)^p = (1+i)i^{(p-1)/2}2^{(p-1)/2}$.

(b) Show that $\left(\frac{2}{p}\right)(1+i)i^{(p-1)/2} \equiv 1 + i(-1)^{(p-1)/2} \pmod p$. Use this to show that $\left(\frac{2}{p}\right) \equiv (-1)^{(p\pm1)/4} \pmod p$ predicated upon whether $\frac{p-1}{2}$ is even or odd.

(c) Deduce that $\left(\frac{2}{p}\right) \equiv (-1)^{(p^2-1)/8}$.

(a) Note $(1+i)^2 = 1 + 2i + i^2 = 1 + 2i - 1 = 2i$, hence

$$(1+i)^p = (1+i)((1+i)^2)^{(p-1)/2} = (1+i)i^{(p-1)/2}2^{(p-1)/2}.$$

(b) Observe, $i^p = i \cdot i^{p-1} = i(-1)^{(p-1)/2}$. Since $(1+i)^p \equiv 1 + i^p \pmod p$ and $2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \pmod p$, we have that $\left(\frac{2}{p}\right)(1+i)i^{(p-1)/2} \equiv 1+i(-1)^{(p-1)/2} \pmod p$ as desired. If $(p-1)/2$ is even, then the congruence becomes $\left(\frac{2}{p}\right)(1+i)(-1)^{(p-1)/4} \equiv 1+i \pmod p$. Since p is odd, $1+i$ is invertible in $(\mathbf{Z}/p\mathbf{Z})[i]$. The congruence is therefore equivalent to $\left(\frac{2}{p}\right) \equiv (-1)^{(p-1)/4} \pmod p$. If $(p-1)/2$ is odd, the congruence becomes $\left(\frac{2}{p}\right)(1+i)i^{(p-1)/2} \equiv 1-i \pmod p$. Multiplying by i, and using the fact that $(p-1)/2$ is odd, the congruence is equivalent to $\left(\frac{2}{p}\right)(1+i)(-1)^{(p+1)/2} \equiv 1+i \pmod p$. Dividing by $1+i$, the congruence is equivalent to $\left(\frac{2}{p}\right) \equiv (-1)^{(p+1)/2}$.

(c) Observe that $\frac{p^2-1}{8} = \frac{p-1}{4}\frac{p+1}{2} = \frac{p+1}{4}\frac{p-1}{2}$. It follows at once that $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Question 5. Use quadratic reciprocity to determine $\left(\frac{3}{p}\right)$.

By quadratic reciprocity, $(3 \mid p) = (-1)^{(p-1)/2}(p \mid 3)$. We next consider the possible cases for the residues of p modulo 4 and 3. Suppose first that $p \equiv 1 \pmod 4$. If $p \equiv 1 \pmod 3$, then $p \equiv 1 \pmod{12}$ and $(3 \mid p) = 1$; if $p \equiv 2 \pmod 3$, then $p \equiv 5 \pmod{12}$ and $(3 \mid p) = -1$. Next, suppose that $p \equiv 3 \pmod 4$. If $p \equiv 1 \pmod 3$, then $p \equiv 7 \pmod{12}$ and $(3 \mid p) = -1$; if $p \equiv 2 \pmod 3$, then $p \equiv 11 \pmod{12}$ and $(3 \mid p) = 1$. We have shown therefore that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$