Theorem 6.19 Fermat's Little Theorem. *Let p be any prime number and suppose that $p \nmid a$ (p does not divide a). Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for any integer b, $b^p \equiv b \pmod{p}$.

Sage. Sage can create all the subgroups of a group, so long as the group is not too large. It can also create the cosets of a subgroup.

Historical Note

Joseph-Louis Lagrange (1736–1813), born in Turin, Italy, was of French and Italian descent. His talent for mathematics became apparent at an early age. Leonhard Euler recognized Lagrange's abilities when Lagrange, who was only 19, communicated to Euler some work that he had done in the calculus of variations. That year he was also named a professor at the Royal Artillery School in Turin. At the age of 23 he joined the Berlin Academy. Frederick the Great had written to Lagrange proclaiming that the "greatest king in Europe" should have the "greatest mathematician in Europe" at his court. For 20 years Lagrange held the position vacated by his mentor, Euler. His works include contributions to number theory, group theory, physics and mechanics, the calculus of variations, the theory of equations, and differential equations. Along with Laplace and Lavoisier, Lagrange was one of the people responsible for designing the metric system. During his life Lagrange profoundly influenced the development of mathematics, leaving much to the next generation of mathematicians in the form of examples and new problems to be solved.

6.4 Reading Questions

1. State Lagrange's Theorem in your own words.
2. Determine the left cosets of $\langle 3 \rangle$ in $\mathbb{Z}_9$.
3. The set $\{(), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a subgroup of S_4. What is its index in S_4?
4. Suppose G is a group of order 29. Describe G.
5. The number $p = 137909$ is prime. Explain how to compute $57^{137909} \pmod{137909}$ without a calculator.

6.5 Exercises

1. Suppose that G is a finite group with an element g of order 5 and an element h of order 7. Why must $|G| \geq 35$?
2. Suppose that G is a finite group with 60 elements. What are the orders of possible subgroups of G?
3. Prove or disprove: Every subgroup of the integers has finite index.
4. Prove or disprove: Every subgroup of the integers has finite order.

5. List the left and right cosets of the subgroups in each of the following.

(a) $\langle 8 \rangle$ in $\mathbb{Z}_{24}$

(b) $\langle 3 \rangle$ in $U(8)$

(c) $3\mathbb{Z}$ in $\mathbb{Z}$

(d) A_4 in S_4

(e) A_n in S_n

(f) D_4 in S_4

(g) $\mathbb{T}$ in $\mathbb{C}^*$

(h) $H = \{(1), (1\,2\,3), (1\,3\,2)\}$ in S_4

6. Describe the left cosets of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$. What is the index of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$?

7. Verify Euler's Theorem for $n = 15$ and $a = 4$.

8. Use Fermat's Little Theorem to show that if $p = 4n + 3$ is prime, there is no solution to the equation $x^2 \equiv -1 \pmod{p}$.

9. Show that the integers have infinite index in the additive group of rational numbers.

10. Show that the additive group of real numbers has infinite index in the additive group of the complex numbers.

11. Let H be a subgroup of a group G and suppose that $g_1, g_2 \in G$. Prove that the following conditions are equivalent.

(a) $g_1 H = g_2 H$

(b) $H g_1^{-1} = H g_2^{-1}$

(c) $g_1 H \subset g_2 H$

(d) $g_2 \in g_1 H$

(e) $g_1^{-1} g_2 \in H$

12. If $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$, show that right cosets are identical to left cosets. That is, show that $gH = Hg$ for all $g \in G$.

13. What fails in the proof of Theorem 6.8 if $\phi : \mathcal{L}_H \to \mathcal{R}_H$ is defined by $\phi(gH) = Hg$?

14. Suppose that $g^n = e$. Show that the order of g divides n.

15. The ***cycle structure*** of a permutation σ is defined as the unordered list of the sizes of the cycles in the cycle decomposition σ. For example, the permutation $\sigma = (1\,2)(3\,4\,5)(7\,8)(9)$ has cycle structure $(2, 3, 2, 1)$ which can also be written as $(1, 2, 2, 3)$.

Show that any two permutations $\alpha, \beta \in S_n$ have the same cycle structure if and only if there exists a permutation γ such that $\beta = \gamma\alpha\gamma^{-1}$. If $\beta = \gamma\alpha\gamma^{-1}$ for some $\gamma \in S_n$, then α and β are ***conjugate***.

16. If $|G| = 2n$, prove that the number of elements of order 2 is odd. Use this result to show that G must contain a subgroup of order 2.

17. Suppose that $[G : H] = 2$. If a and b are not in H, show that $ab \in H$.

18. If $[G : H] = 2$, prove that $gH = Hg$.

19. Let H and K be subgroups of a group G. Prove that $gH \cap gK$ is a coset of $H \cap K$ in G.

20. Let H and K be subgroups of a group G. Define a relation $\sim$ on G by $a \sim b$ if there exists an $h \in H$ and a $k \in K$ such that $hak = b$. Show that this relation is an equivalence relation. The corresponding equivalence classes are called ***double cosets***. Compute the double cosets of $H = \{(1), (1\,2\,3), (1\,3\,2)\}$ in A_4.

21. Let G be a cyclic group of order n. Show that there are exactly $\phi(n)$ generators for G.

22. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes. Prove that

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

23. Show that

$$n = \sum_{d|n} \phi(d)$$

for all positive integers n.