Section IV.20. Fermat's and Euler's Theorems

Note. The results of this section really belong in a class on number theory. The results relate to modular arithmetic. We have seen that the cyclic groups $\mathbb{Z}_n$ and the fields $\mathbb{Z}_p$ where p is prime, are of particular interest, so the relevance of modular arithmetic should not be a huge surprise.

Exercise 18.37. Let $\langle R, +, \cdot \rangle$ be a ring with unity and let U be the set of all units in R. Then $\langle U, \cdot \rangle$ is a group.

Proof. First, we show that U is closed under $\cdot$. Let $u, v \in U$. Then for some $u', v' \in U$ we have $u \cdot u' = u' \cdot u = 1$ and $v \cdot v' = v' \cdot v = 1$. Then

$$(v' \cdot u') \cdot (u \cdot v) = v'(u'u)v = v'1v = v'v = 1,$$

and

$$(u \cdot v) \cdot (v' \cdot u') = u(vv')u' = u1u' = uu' = 1.$$

So $uv \in U$ and U is closed under $\cdot$. Associativity of $\cdot$ is inherited from R ($\mathcal{G}_1$). Since $1 \cdot 1 = 1$, then $1 \in U$ ($\mathcal{G}_2$). For $u \in U$, there is $u' \in U$ as above where $u \cdot u' = 1$ ($\mathcal{G}_2$). Therefore, $\langle U, \cdot \rangle$ is a group. ∎

Corollary. For any field, the nonzero elements form a group under the field multiplication.

Proof. In a field, all nonzero elements are units. So this follows from Exercise 18.37. ∎

Theorem 20.1. Little Theorem of Fermat.

If $a \in \mathbb{Z}$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$. That is, $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$.

Corollary 20.2. If $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$ for any prime p.

Exercise 20.4. Use Fermat's theorem to find the remainder of 3^{47} when it is divided by 23.

Solution. Since $p = 23$ is prime, we use Fermat's Theorem to deal with $p - 1 = 22$ order powers of 3.

$$3^{47} = 3^{22} \cdot 3^{22} \cdot 3^3 \equiv (1)(1)3^3 \pmod{23} = 27 \pmod{23} \equiv 4 \pmod{23}.$$

So the remainder is 4.

Theorem 20.6. The set G_n of nonzero elements of $\mathbb{Z}_n$ that are not 0 divisors forms a group under multiplication modulo n.

Definition. For $n \in \mathbb{N}$, define $\phi(n)$ as the number of natural numbers less than or equal to n which are relatively prime to n. ϕ is the *Euler phi-function*.

Example. $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(12) = 4$, and $\phi(p) = p - 1$ for p prime.

Note. The group G_n of Theorem 20.6 is abelian and is order $\phi(n)$. You might wonder if these are "new" groups to us. However, since G_n is a finite abelian group, then we know that we have already encountered it in the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 11.12).

Theorem 20.8. Euler's Theorem.
If a is an integer relatively prime to n, then $a^{\phi(n)} - 1$ is divisible by n. That is, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Exercise 20.10. Use Euler's Theorem to find the reminder of 7^{1000} when divided by 24.

Solution. Notice $\phi(24) = 8$ (1, 5, 7, 11, 13, 17, 19, and 23 are relatively prime to 24), so

$$7^{1000} = (7^8)^{125} \equiv (1)^{125} \pmod{24} \equiv 1 \pmod{24}.$$

The remainder is 1. (Also, $7^2 = 49 \equiv 1 \pmod{24}$, and $7^{1000} = (7^2)^{500} \equiv (1)^{500} \pmod{24} \equiv 1 \pmod{24}$.)

Note. We are ultimately interested in solving algebraic equations. The simplest is $ax = b$. The following results deal with solutions to this equation.

Theorem 20.10. Let m be a positive integer and let $a \in \mathbb{Z}_m$ be relatively prime to m. For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has a unique solution in $\mathbb{Z}_m$.

Corollary 20.11. If a and m are relatively prime integers, then for any integer b, the congruence $ax = b \pmod{m}$ has as solutions all integers in precisely one residue class modulo m.

Theorem 20.12. Let m be a natural number and let $a, b \in \mathbb{Z}_m$. Let $d = \gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and only if d divides b. When d divides b, the equation has exactly d solutions in $\mathbb{Z}_m$.

Corollary 20.13. Let $d = \gcd(a, m)$. The congruence $ax = b \pmod{m}$ has a solution if and only if d divides b. When this is the case, the solutions are the integers in exactly d distinct residue classes modulo m.

Exercise 20.18. Find all solutions to $39x \equiv 52 \pmod{130}$.

Solution. In the notation of Theorem 20.12 we have $d = \gcd(a, m) = \gcd(39, 130) = 13$. Now d divides b (i.e., 13 divides 52) so there is a solution. We consider the "new" equation which results from dividing out factors of $d = 13$, $3x \equiv 4 \pmod{10}$ (this is equation $a_1 x \equiv b_1 \pmod{m_1}$ in the proof of Theorem 20.12). Now 7 is the multiplicative inverse of 3 modulo 10, so $3x \equiv 4 \pmod{10}$ if and only if $7 \cdot 3x \equiv 7 \cdot 4 \pmod{10}$, or $x \equiv 8 \pmod{10}$. So the set of all solutions in $\mathbb{Z}_{130}$ of $39x \equiv 52 \pmod{130}$ is $\{8, 18, 28, 38, \ldots, 118, 128\}$. The solution set of all solutions in $\mathbb{Z}$ contains the following residue classes:

$$\begin{aligned} 8 + 130\mathbb{Z} &= \{\ldots, -122, 8, 138, 268, \ldots\}, \\ 18 + 130\mathbb{Z} &= \{\ldots, -112, 18, 148, 278, \ldots\}, \\ &\vdots \\ 128 + 130\mathbb{Z} &= \{\ldots, -132, -2, 128, 268, \ldots\}. \end{aligned}$$