Math 345-60 Abstract Algebra I

Questions for Section 20: Fermat’s and Euler’s Theorem

1. Some preliminaries: let us carefully work out the addition and multiplication table for the ring \( \mathbb{Z}/n\mathbb{Z} \). By definition, this set consists of the cosets \([a] = a + n\mathbb{Z} = \{a + nk : k \in \mathbb{Z}\} \). We will define \([a] + [b] = [a + b]\) and \([a][b] = [ab]\). We must be careful to verify that these operations are well-defined. For example, if \( n = 5 \) then we have \([2] = [7] \) and \([4] = [-1]\), so we should have \([2 + 4] = [7 + (-1)]\) and \([2 \cdot 4] = [7 \cdot (-1)]\). We will verify this in the abstract. Also, note that \([a] + [b] - [a] = 2\). First, we’ll show that if \( a \) and \( b \) are distinct elements of \( \mathbb{Z}/n\mathbb{Z} \) then \( a + b = a' + b' \) if and only if \( p - q \) is divisible by \( n \). Reason: \([p] = [q] \iff p \in [q] \iff p = q + nk \iff n|p - q\). Note also that if \( 0 \leq a < b < n \) then \([a] = [b]\) implies \( n|(a - b) \) implies \( a - b = 0 \) implies \( a = b \). So the distinct elements of \( \mathbb{Z}/n\mathbb{Z} \) are \([0],[1],\ldots,[n-1]\).

2. First, we’ll show that if \([a] = [a']\) and \([b] = [b']\) then \([a] + [b] = [a'] + [b']\). We need only verify that \( n \) divides \( a + b - a' - b' \). We have \( a - a' = nj \) and \( b - b' = nk \), therefore \( a + b - a' - b' = n(j + k)\).

3. Second, we’ll show that \([ab] = [a'b']\). We have \( a - a' = nj \) and \( b - b' = nk \), therefore \( ab - a'b' = ab - a'b + a'b - a'b' = n(jb + a'k)\).

4. Theorem 20.6: Let \( G_n \) denote the subset of \( \mathbb{Z}/n\mathbb{Z} \) defined by \( G_n = \{[a] : \gcd(a,n) = 1\} \). For example, \( G_{12} = \{[1],[5],[7],[11]\}\). Then \( G_n \) is an abelian group under multiplication of cosets.

**Proof:** First, we’ll show that \( G_n \) is closed with respect to multiplication. Suppose that \([a] \in G_n \) and \([b] \in G_n \). Then \( \gcd(a,n) = \gcd(b,n) = 1 \). Therefore we can find \( p, q, r, s \in \mathbb{Z} \) such that \( pa + qn = rb + sn = 1 \). Therefore \( 1 = (pa+qn)(rb+sn) = pr(ab) + (pas+qnr+qns)n \), therefore \( \gcd(ab,n) = 1 \), therefore \([a][b] = [ab] \in G_n \). We have \([a][b] = [ab] = [ba] = [b][a]\) for all \([a],[b] \in G_n \). Next, we’ll argue that multiplication is associative in \( G_n \). We have \([a]([b][c]) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c]\). Since \( \gcd(1,n) = 1 \), \([1] \in G_n \), and this is the identity element \( e \) in \( G_n \). Finally, we show that for each \([a] \in G_n \) there exists \([b] \in G_n \) such that \([a][b] = [b][a] = e = [1]\). Using \( pa + qn = 1 \), we can see that \( \gcd(p,n) = 1 \) and that \( pa - 1 = n(-q) \) is divisible by \( 1 \). Therefore \([p][a] = [pa] = [1]\).

5. Note: \( G_n \) is a finite group. To see this, let \([a] \in G_n \) be given. Write \( a = nq + r, \ 0 \leq r < n \) by the division algorithm. Then \( a - r = nq \) is divisible by \( n \), therefore \([a] = [r]\). Note that \( \gcd(a,n) = 1 \implies pa + qn = 1 \implies [a] \in G_n \).
The notation for $|G_n|$ is $\phi(n)$, the number of positive integers $\leq n$ which are relatively prime to $n$. For example, $\phi(12) = 4$.

6. **Euler’s Theorem (20.8):** If $a$ is an integer relatively prime to $n$ then $a^{\phi(n)} - 1$ is divisible by $n$.

**Proof:** In $G_n$ we have $[a^{\phi(n)}] = [a]^{\phi(n)} = [a]^{[G_n]} = e = [1]$, therefore $a^{\phi(n)} - 1$ is divisible by $n$.

Example: $n = 12$, $a = 7$, $\phi(12) = 4$ and $a^{\phi(n)} - 1 = 7^4 - 1 = 2400 = 200 \cdot 12$.

7. **Little Theorem of Fermat (20.1):** If $a \in \mathbb{Z}$ and $p$ is a prime not dividing $a$, then $p$ divides $a^{p-1} - 1$.

**Proof:** $a$ is relatively prime to $p$. $\phi(p) = p - 1$. Now use Euler’s Theorem.

8. **Example 20.5:** For each $n \in \mathbb{Z}$, $n^{33} - n$ is divisible by 15. **Proof:** Suppose that $n^{33} - n$ is not divisible by 15. Then $n$ is not divisible by 15. Therefore $n$ is not divisible by 3 or not divisible by 5. Suppose $n$ is not divisible by 3. Then it is relatively prime to 3 since 3 is prime. Therefore $n^2 - 1$ is divisible by 3, therefore $[n^2] = [1]$ in $\mathbb{Z}/3\mathbb{Z}$, therefore $[n^{33}] = [n][n^2]^{16} = [n][1]^{16} = [n]$, therefore 3 divides $n^{33} - n$, therefore 15 divides $n^{33} - n$: contradiction. So $n$ must not be divisible by 5. Then it is relatively prime to 5 since 5 is prime. Therefore $n^4 - 1$ is divisible by 5, therefore $[n^4] = [1]$ in $\mathbb{Z}/5\mathbb{Z}$, therefore $[n^{33}] = [n][n^4]^8 = [n][1]^8 = [n]$, therefore 5 divides $n^{33} - n$, therefore 15 divides $n^{33} - n$: contradiction. So $n^{33} - n$ must be divisible by 15. For example, $2^{33} - 2 = 8589934590 = 15 \cdot 572662306$.

9. **Corollary 20.13:** The congruence $ax \equiv b \mod m$ has a solution $x$ if and only $d | b$, where $d = \gcd(a, m)$. If $d | b$, then there are exactly $d$ possibilities for $[x]$ in $G_m$.

**Proof:** Suppose $ax \equiv b \mod m$ has a solution $x$. This means that $ax - b$ is divisible by $m$, hence divisible by $d$, which implies $[ax] = [b]$ in $\mathbb{Z}/d\mathbb{Z}$. Since $a - 0$ is divisible by $d$, $[a] = [0]$, therefore $[b] = [ax] = [a][x] = [0][x] = [0]$, therefore $b - 0$ is divisible by $d$. Conversely, suppose $b$ is divisible by $d$. Write $a = a_0d$, $m = m_0d$, $b = b_0d$. We know that $\gcd(a_0, m_0) = 1$, therefore $ra_0 + sm_0 = 1$ for some $r, s \in \mathbb{Z}$. Multiplying this through by $b = b_0d$, we obtain $ra_0b_0d + sm_0b_0d = b$, i.e. $arb_0 + msb_0 = b$, i.e. $a(rb_0) - b = m(-sb_0)$. 

$p(nq + r) + qn = 1 \Rightarrow pr + (pq + q)n = 1 \Rightarrow \gcd(r, n) = 1$. So the elements in $G_n$ can be represented by $[r], 0 \leq r < n$, which satisfy $\gcd(r, n) = 1$. Note that this does not include $r = 0$, because $\gcd(0, n) = n$ and $n > 1$ in general.
Therefore, setting $x = rb_0$, we see that $ax - b$ is divisible by $m$, hence $ax \equiv b \mod m$.

Now assume that there is at least one solution to $ax \equiv b \mod m$. We will count the number of solutions modulo $m$, i.e. the distinct solutions to $[a][x] = [b]$ in $\mathbb{Z}/m\mathbb{Z}$. First, we know that $a = a_0d$ and $b = b_0d$, so we will express this as $[a_0d][x] = [b_0d]$. $[x]$ is a solution if and only if $a_0dx - b_0d$ is divisible by $m$ if and only if $a_0x - b_0$ is divisible by $m_0$ if and only if $[a_0][x] = [b_0]$ in $\mathbb{Z}/m_0\mathbb{Z}$. So when can $[a_0][x] = [a_0][y]$ in $\mathbb{Z}/m_0\mathbb{Z}$? Answer: when $m_0|(a_0x - a_0y)$. That is, when $m_0|a_0(x - y)$. Since $m_0$ and $a_0$ are relatively prime, this can only occur when $m_0|(x - y)$. Let $x$ be the smallest solution in the range $\{0, 1, \ldots, m - 1\}$. Then solutions $\geq$ this are $x, x + m_0, x + 2m_0, \ldots$. We must count how many of these solutions lie in $\{0, 1, \ldots, m - 1\}$. First note that $x < m_0$, otherwise $y = x - m_0$ is a smaller solution in $\{0, 1, \ldots, m - 1\}$. Therefore $x + (d - 1)m_0 = x + m - m_0 < m$ is a solution. Hence we have at least $d$ distinct solutions, namely $x, x + m_0, \ldots, x + (d - 1)m_0$. The next largest solution is $x + dm_0 = x + m$, which does not belong to $\{0, 1, \ldots, m - 1\}$. So there are exactly $d$ solutions for $x$.

10. See Examples 20.14 and 20.15, page 188.

**Homework for Section 20, due ??? (only the starred problems will be graded):**

$7^*, 8^*, 9^*, 10^*, 15^*, 17^*, 29^*, 30^*$

Hints:

10. This is the same as computing $[7^{1000}] = [7]^{1000}$ in $\mathbb{Z}/24\mathbb{Z}$ and reducing it to $[r]$ where $0 \leq r < 24$. You will need to compute $\phi(24)$. Then Euler’s Theorem says $[7]^{\phi(24)} = [1]$. You can use this result to simplify $[7]^{1000}$.

29. Similar to Example 20.5, page 185 (see also Comment 8 in the notes above).

30. Find a suitable prime number $p$, different from the divisors of 383838, such that $n^{37} - n$ is divisible by $p$. Then it will be divisible by all the divisors of 383838 and divisible by $p$, and since these are distinct primes, the Fundamental Theorem of Arithmetic says that the product of all these primes divides $n^{37} - n$. That is, 383838$p$ divides $n^{37} - n$. 

3