Math 461 **Spring 2015**
Homework 5 **Drew Armstrong**

---

1. Equivalence mod n. Let S be a set. For each pair $(x, y) \in S^2$ we define $x \sim y$ to be either true or false, and we will usually write $x \sim y$ as shorthand for "$x \sim y$ is true". We say that $\sim$ is an **equivalence relation** if

- $x \sim x$ for all $x \in S$,
- $x \sim y$ implies $y \sim x$ for all $x, y \in S$,
- $x \sim y$ and $y \sim z$ imply $x \sim z$ for all $x, y, z \in S$.

Now let $n \in \mathbb{Z}$ be a **nonzero** integer. For all $x, y \in \mathbb{Z}$ we will write $x \sim_n y$ to mean that n divides $x - y$ (i.e., there exists $k \in \mathbb{Z}$ such that $x - y = nk$). Prove that $\sim_n$ is an equivalence relation on $\mathbb{Z}$.

Proof. First, consider any integer $x \in \mathbb{Z}$. Since $x - x = 0 = n \cdot 0$ we conclude that $x \sim_n x$.

Second, consider any integers $x, y \in \mathbb{Z}$ and assume that $x \sim_n y$, i.e., assume that there exists $k \in \mathbb{Z}$ such that $x - y = nk$. Then we have $y - x = -(x - y) = -nk = n(-k)$, and hence $y \sim_n x$.

Third, consider any integers $x, y, z \in \mathbb{Z}$ and assume that $x \sim_n y$ and $y \sim_n z$. In other words, assume that there exist $k, \ell \in \mathbb{Z}$ such that $x - y = nk$ and $y - z = n\ell$. Adding these two equations gives

$$x - z = (x - y) + (y - z) = nk + n\ell = n(k + \ell),$$

hence $x \sim_n z$. We conclude that $\sim_n$ is an equivalence relation on $\mathbb{Z}$.

$\square$

2. Primitive Roots of Unity. Consider a positive integer $n \in \mathbb{Z}$ and let $\omega = e^{2\pi i/n}$.

(a) Prove that $\omega^k = \omega^\ell$ if and only if $k \sim_n \ell$ (as in Problem 1).
(b) Given an integer k, let m be the smallest positive integer such that $(\omega^k)^m = 1$. Show that $m = \mathrm{lcm}(k, n)/k$.
(c) Prove that ω^k is a primitive nth root of 1 if and only if $\gcd(k, n) = 1$. [Hint: $\gcd(k, n) = kn/\mathrm{lcm}(k, n)$.]

Proof. For part (a), first recall that $e^{i\theta} = 1$ if and only if $\theta = 2\pi m$ for some $m \in \mathbb{Z}$. Then

$$\begin{aligned}
\omega^k = \omega^\ell &\Longleftrightarrow \omega^k/\omega^\ell = 1 \\
&\Longleftrightarrow \omega^{k-\ell} = 1 \\
&\Longleftrightarrow e^{2\pi i(k-\ell)/n} = 1 \\
&\Longleftrightarrow 2\pi(k - \ell)/n = 2\pi m \text{ for some } m \in \mathbb{Z} \\
&\Longleftrightarrow k - \ell = nm \text{ for some } m \in \mathbb{Z} \\
&\Longleftrightarrow k \sim_n \ell.
\end{aligned}$$

For part (b), let m be the **smallest positive integer** such that $(\omega^k)^m = 1$. Note from part (a) that

$$\begin{aligned}(\omega^k)^m = 1 &\iff \omega^{km} = 1\\ &\iff \omega^{km} = \omega^0\\ &\iff km \sim_n 0\\ &\iff km = n\ell \text{ for some } \ell \in \mathbb{Z}\\ &\iff km \text{ is a multiple of } n\\ &\iff km \text{ is a common multiple of } k \text{ and } n.\end{aligned}$$

The last equivalence is true because km is always a multiple of k so this condition is vacuous. If m is the **smallest positive integer** such that km is a common multiple of k and n, then clearly km must be the **least common multiple** of k and n. We conclude that

$$\begin{aligned}km &= \mathrm{lcm}(k,n)\\ m &= \frac{1}{k}\mathrm{lcm}(k,n).\end{aligned}$$

For part (c) we recall (or assume, if we don't recall) that

$$\begin{aligned}nk &= \mathrm{lcm}(k,n)\cdot\gcd(k,n)\\ nk/\mathrm{lcm}(k,n) &= \gcd(k,n).\end{aligned}$$

Also, we recall the definition of primitive roots: Every nth root of 1 has the form ω^k for some $k \in \mathbb{Z}$. We say that ω^k is a **primitive** nth root of 1 if the **smallest positive integer** m such that $(\omega^k)^m = 1$ is $m = n$. Thus from part (b) we have

$$\begin{aligned}\omega^k \text{ is primitive } &\iff n = \frac{1}{k}\mathrm{lcm}(k,n)\\ &\iff nk/\mathrm{lcm}(k,n) = 1\\ &\iff \gcd(k,n) = 1.\end{aligned}$$

$\square$

3. Euler's Totient Function. Given a positive integer $n \in \mathbb{Z}$ we define

$$\varphi(n) := \#\{k : 0 \leq k \leq n-1, \gcd(k,n) = 1\}.$$

(a) Explain why $\varphi(n)$ is the degree of the cyclotomic polynomial $\Phi_n(x) \in \mathbb{Z}[x]$.

(b) If $p \in \mathbb{Z}$ is prime and m is a positive integer, prove that $\varphi(p^m) = p^m - p^{m-1}$. [Hint: The only integers less than p^m that are not coprime to p^m are the multiples of p. How many of these are there?]

(c) Prove that for all positive integers n we have

$$\varphi(n) = n\prod_{p|n}\frac{p-1}{p},$$

where the product is over prime numbers p that divide n. [Hint: You can assume without proof that for all coprime $a,b \in \mathbb{Z}$ we have $\varphi(ab) = \varphi(a)\varphi(b)$. Now express n as a product of primes $n = p_1^{m_1}p_2^{m_2}\cdots$.]

(d) Compute the degree of $\Phi_{120}(x)$. Do not compute $\Phi_{120}(x)$ itself.

Proof. For part (a), recall that the nth cyclotomic polynomial is given by

$$\Phi_n(x) = \prod_{\zeta}(x - \zeta)$$

where ζ runs over the primitive nth roots of unity. From Problem 2(c) we know that the number of primitive nth roots of unity is $\varphi(n)$. Let $\zeta_1, \zeta_2, \ldots, \zeta_{\varphi(n)}$ be the primitive roots. Then by the additivity of degree we have

$$\begin{aligned}
\deg \Phi_n(x) &= \deg(x - \zeta_1)(x - \zeta_2)\cdots(x - \zeta_{\varphi(n)}) \\
&= \deg(x - \zeta_1) + \deg(x - \zeta_2) + \cdots + \det(x - \zeta_{\varphi(n)}) \\
&= \underbrace{1 + 1 + \cdots + 1}_{\varphi(n) \text{ times}} \\
&= \varphi(n).
\end{aligned}$$

For part (b), let p be prime and let m be a positive integer. To compute $\varphi(p^m)$ we must count the integers less than p^m that are coprime to p^m. In this case it turns out to be easier to count the integers that are **not** coprime to p^m: these are just the multiples of p (any number that is not a multiple of p is necessarily coprime to p^m because p is the only prime factor of p^m). The multiples of p from $1 \cdot p$ up to $p^m = p^{m-1} \cdot p$ are

$$1 \cdot p,\ 2 \cdot p,\ 3 \cdot p, \ldots, (p^{m-1} - 1) \cdot p,\ p^{m-1} \cdot p$$

and there are p^{m-1} of these. Subtracting these from the p^m numbers $1, 2, 3, \ldots, p^m$ gives

$$\varphi(p^m) = p^m - p^{m-1}.$$

For part (c), we can factor n as

$$n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$$

where $p_1, p_2, \ldots, p_k$ are the distinct prime factors of n. Then we use the fact that φ multiplies over coprime factors [we'll just assume this fact; if you want to look it up, it's called the "Chinese remainder theorem"] we get

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}) \\
&= \varphi(p_1^{m_1})\varphi(p_2^{m_2}) \cdots \varphi(p_k^{m_k}) \\
&= (p_1^{m_1} - p_1^{m_1 - 1})(p_2^{m_2} - p_2^{m_2 - 1}) \cdots (p_k^{m_k} - p_k^{m_k - 1}) \\
&= p_1^{m_1}\left(\frac{p_1 - 1}{p_1}\right) p_2^{m_2}\left(\frac{p_2 - 1}{p_2}\right) \cdots p_k^{m_k}\left(\frac{p_k - 1}{p_k}\right) \\
&= p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}\left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right) \cdots \left(\frac{p_k - 1}{p_k}\right) \\
&= n\left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right) \cdots \left(\frac{p_k - 1}{p_k}\right) \\
&= n\prod_{i=1}^{k}\left(\frac{p_i - 1}{p_i}\right)
\end{aligned}$$

which is just what we wanted to show.

For part (d), we will apply the formula from part (c) to compute $\varphi(120)$. Note that $120 = 2^3 \cdot 3 \cdot 5$, so the prime factors are 2, 3, and 5. Then the formula says

$$\begin{aligned}
\varphi(120) &= 120\left(\frac{2-1}{2}\right)\left(\frac{3-1}{3}\right)\left(\frac{5-1}{5}\right) \\
&= 120\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) \\
&= 32.
\end{aligned}$$

We conclude that there are 32 primitive 120th roots of unity, and hence $\deg \Phi_{120}(x) = 32$. Note that since $\varphi(120) = 32 = 2^5$ is a power of 2, the Gauss-Wantzel Theorem tells us that the regular 120-gon **is** constructible with straightedge and compass. □

[For the curious, my computer told me that $\Phi_{120}(x) = x^{32} + x^{28} - x^{20} - x^{16} - x^{12} + x^4 + 1$ and

$$\begin{aligned}
x^{120} - 1 = (x-1)&(1+x^4+x^3+x^2+x)(1+x^2+x)(1-x+x^3-x^4+x^5-x^7+x^8)(1+x) \\
&(1-x+x^2-x^3+x^4)(1-x+x^2)(x^8+x^7-x^5-x^4-x^3+x+1)(1+x^2) \\
&(x^8-x^6+x^4-x^2+1)(x^4-x^2+1)(x^{16}+x^{14}-x^{10}-x^8-x^6+x^2+1) \\
&(1+x^4)(x^{16}-x^{12}+x^8-x^4+1)(x^8-x^4+1)(x^{32}+x^{28}-x^{20}-x^{16}-x^{12}+x^4+1).
\end{aligned}$$

Obviously I would never compute that by hand.]

4. Fermat Primes. In 1650, Pierre de Fermat conjectured that every number of the form $F(n) = 2^{2^n} + 1$ is prime. He based this conjecture on the fact that $F(0) = 3, F(1) = 5, F(2) = 17, F(3) = 257, F(4) = 65537$ are prime. However, Euler showed in 1732 that $F(5)$ is **not** prime, and to this day it is not known whether there exist **any** other "Fermat primes". D'oh!

(a) If $2^a + 1$ is a prime number, prove that a must be a power of 2. [Hint: Suppose that $a = bc$ where b is **odd**. Factor the polynomial $1 - x^b$ and then substitute $x = -2^c$.]

(b) Let p be prime. If $\varphi(p)$ is a power of two, show that p is a Fermat prime.

Proof. For part (a) we will prove the contrapositive statement, i.e., we will prove that if a is **not** a power of 2 then $2^a + 1$ is **not** prime. So assume that a is not a power of 2. This means that a must have an odd factor, say $a = bc$ where b is odd and c is arbitrary. In this case we will show that the number $2^a + 1$ can be factored. Indeed, note that the polynomial $1 - x^b$ factors as

$$1 - x^b = (1-x)(1 + x + x^2 + x^3 + \cdots + x^{b-1}).$$

Then substituting $x = -2^c$ (and using the fact that b is odd) gives

$$\begin{aligned}
1 - (-2^c)^b &= (1+2^c)(1 + (-2^c) + (-2^c)^2 + (-2^c)^3 + \cdots + (-2^c)^{b-1}) \\
1 - (-1)^b 2^{bc} &= (1+2^c))(1 - (-1)^c 2^c + (-1)^2 2^{2c} + (-1)^3 2^{3c} + \cdots (-1)^{b-1} 2^{(b-1)c}) \\
1 + 2^a &= (1+2^c)(1 - 2^c + 2^{2c} - 2^{3c} + \cdots + 2^{(b-1)c})
\end{aligned}$$

Since $1 + 2^c$ is not equal to 1 or to $1 + 2^a$ we conclude that $1 + 2^a$ is not prime.

For part (b), let p be prime and suppose that $\varphi(p) = 2^k$ for some k. From Problem 3(b) we know that $\varphi(p) = p - 1$, hence

$$\begin{aligned}
\varphi(p) &= 2^k \\
p - 1 &= 2^k \\
p &= 2^k + 1.
\end{aligned}$$

We conclude that p is a Fermat prime. □