Kris Harper
MATH 24200
April 19, 2010

Homework 2

Problem 1. *Show that there are infinitely many primes congruent to* -1 *modulo* 6.

Proof. Suppose there are finitely many such, $p_1, \ldots, p_n$ and let $m = 3p_1 \ldots p_n + 2$. Then $m \equiv -1 \pmod 6$. Assume that m is not prime so that $m = q_1 \ldots q_k$ with q_i prime. Note that $3 \nmid m$ since $m \equiv 2 \pmod 3$ and no q_i is congruent to -1 modulo 6 because m is not a multiple of any p_i. Then every q_i is congruent to 1 modulo 6 so $m \equiv 1 \pmod 6$, a contradiction. Thus there must be infinitely many primes congruent to -1 modulo 6. □

Problem 2. *Show that the equation* $3x^2 + 2 = y^2$ *has no integer solutions.*

Proof. If we reduce modulo 3 we're left with $2 \equiv y^2 \pmod 3$. But $1^2 \equiv 2^2 \equiv 1 \pmod 2$ so there are no integers y such that $y^2 \equiv 2 \pmod 3$. □

Problem 3. *Extend the notion of congruence to the ring* $\mathbb{Z}[i]$ *and prove that* $a + bi$ *is always congruent to* 0 *or* 1 *modulo* $1 + i$.

Proof. The definition will be the same as that of $\mathbb{Z}$. Namely, $a + bi \equiv c + di \pmod{m + ni}$ if there exists $e + fi \in \mathbb{Z}[i]$ such that $(e + fi)(m + ni) = (a + bi) - (c + di)$.

Now note that $(e + fi)(1 + i) = (e - f) + (e + f)i$. Without loss of generality assume $a < b$. Let $k = 2((b - a)/2 - [(b - a)/2])$ so that k is 0 if $b - a$ is even and 1 if $b - a$ is odd. Now let $f = [b - a/2]$ and $e = a + f + k$. Then $e + f = b$ and $e - f$ is either a or $a + 1$ depending on k. Thus $(e + fi)(i + 1) = (a + bi)$ or $(e + fi)(i + 1) = (a + bi) - 1$ so that $a + bi \equiv 0 \pmod{1 + i}$ or $a + bi \equiv 1 \pmod{1 + i}$. □

Problem 4. *Extend the notion of congruence to* $\mathbb{Z}[\omega]$ *and prove that* $a + b\omega$ *is always congruent to either* -1, 1 *or* 0 *modulo* $1 - \omega$.

Proof. The definition of congruence is exactly like that in Problem 3. Let $a + b\omega \in \mathbb{Z}[\omega]$ and suppose $(e+f\omega)(1-\omega) = (a+b\omega)-(c+d\omega)$. Note that $(e+f\omega)(1-\omega) = (e+f)+(2f-e)\omega$. Choose $f = [(a+b)/3]$ and $e = a - f + k$ where $k = 0$ if $a + b \equiv 0 \pmod 3$, $k = 1$ if $a + b \equiv 1 \pmod 3$ and $k = -1$ if $a + b \equiv -1 \pmod 3$. Then $b = 2f - e$ and $a = e + f$ or $a = e + f \pm 1$ depending on the value of k. Thus $(e + f)(1 - \omega) = a + b\omega$ or $(e + f)(1 - \omega) = (a + b\omega) \pm 1$. Thus $a + b\omega$ is congruent to either 0, 1 or -1 modulo $1 - \omega$. □

Problem 5. *Let* $\lambda = 1 - \omega \in \mathbb{Z}[\omega]$. *If* $\alpha \in \mathbb{Z}[\omega]$ *and* $\alpha \equiv 1 \pmod \lambda$, *prove that* $\alpha^3 \equiv 1 \pmod 9$.

Proof. We can write $\alpha = 1+\beta\lambda$ so that $\alpha^3 = 1+3\beta\lambda+3\beta^2\lambda^2+\beta^3\lambda^3$. Note also that $-\omega^2\lambda^2 = -\omega^2(1-\omega)^2 = -\omega^2(1-2\omega+\omega^2) = -\omega^2(-3\omega) = 3$. Putting this in the first equation we have $\alpha^3 = 1-\beta\omega^2\lambda^3-\beta^2\omega^2\lambda^4+\beta^3\lambda^3$. Reducing modulo λ^4 we have $\alpha^3 \equiv 1 + (\beta^3 - \beta\omega^2)\lambda^3 \pmod{\lambda^4}$. But note that $\lambda \mid \beta^3 - \beta\omega^2$ so this equation reduces to $\alpha^3 \equiv 1 \pmod{\lambda^4}$. By the above statement $9 \mid \lambda^4$ so we're done. □

Problem 6. *Use Exercise 25 to show that if* $\xi, \eta, \zeta \in \mathbb{Z}[\omega]$ *are not zero and* $\xi^3 + \eta^3 + \zeta^3 = 0$ *then* λ *divides at least one of the elements* ξ, η, ζ.

Proof. From Problem 4 we know that each of ξ, η and ζ is congruent to either -1, 1 or 0 modulo λ. Moreover, from Problem 5 we know that if any one of ξ, η or ζ is congruent to 1 modulo λ then it's cube also congruent to 1 modulo 9. Therefore it's not possible that all three of these are congruent to 1 modulo λ because otherwise $\xi^3 + \eta^3 + \zeta^3 \equiv 3 \pmod 9$. It's also not possible that any two of these are congruent to 1 modulo λ since then the congruence of the cubic sum would be at least 1. So at most 1 of ξ, η or ζ can be congruent to 1 modulo λ. Since the congruences must sum to 0 we can either have one value congruent to 1, one value congruent to -1 and one value congruent to 0, or all three congruent to 0. In either case we have at least one value congruent to 0 which means λ divides at least one value. □

Problem 7. *Suppose that a is a primitive root modulo p^n, p and odd prime. Show that a is a primitive root modulo p.*

Proof. Let n be the order of a modulo p. We can write $a^n = 1+mp$ for some m. Then $a^{np^{n-1}} = (1+mp)^{p^{n-1}} = 1 + p^{n-1}mp + \cdots$ where we've expanded using the binomial theorem. Reducing this equation modulo p^n we have $a^{np^{n-1}} \equiv 1 \pmod{p^n}$. Since a is a primitive root modulo p^n we must have $np^{n-1} = \phi(p^n) = p^{n-1}(p-1)$. Therefore $n = p-1$ and a is a primitive root modulo p. □

Problem 8. *Consider a prime p of the form $4t+1$. Show that a is a primitive root modulo p iff $-a$ is a primitive root modulo p.*

Proof. If a is a primitive root modulo p then a has order $\phi(p) = 4t$ modulo p. Let n be the order of $-a$ modulo p and suppose $n < 4t$. Note $(-a)^n \equiv (-1)^n a^n \equiv 1 \pmod{p}$. Thus n must be odd otherwise $(-1)^n = 1$. But then $(-a)^{2n} \equiv (-1)^{2n}a^{2n} \equiv a^{2n} \equiv 1 \pmod{p}$. But since n is odd $4 \nmid 2n$ and since a has order $4t$ modulo p we have a contradiction. Thus the order of $-a$ modulo p is $4t$ and $-a$ is a primitive root modulo p.

Now suppose $-a$ is a primitive root modulo p so that the order of $-a$ modulo p is $4t$. Let n be the order of a modulo p. Then $a^n \equiv 1 \pmod{p}$ and $1 \equiv a^{2n} \equiv (-1)^{2n}a^{2n} \equiv (-a)^{2n} \pmod{p}$. Thus $4t \mid 2n$ and n must be even. But then $a^n \equiv (-1)^n a^n \equiv (-a)^n \pmod{p}$ and we see that $n = 4t$ is the order of a modulo p so a is a primitive root modulo p. □

Problem 9. *Consider a prime p of the form $4t+3$. Show that a is a primitive root modulo p iff $-a$ has order $(p-1)/2$.*

Proof. Suppose a is a primitive root modulo p so that the order of a modulo p is $\phi(p) = 4t+2 = 2(2t+1)$. Let n be the order of $-a$ modulo p and suppose $n < 4t+2$. Then $(-a)^n \equiv (-1)^n a^n \equiv 1 \pmod{t}$ so that n must be odd otherwise $(-1)^n = 1$. Then $(-a)^{2n} \equiv a^{2n} \equiv 1 \pmod{p}$ so $4t+2 \mid 2n$ and $2t+1 \mid n$. This shows that either $n = 2t+1$ or $n = 4t+2$ and since n is odd we must have $n = 2t+1$ so that the order of $-a$ modulo p is $2t+1 = (p-1)/2$.

Now suppose $-a$ has order $(p-1)/2 = 2t+1$ modulo p so that $(-a)^{2t+1} \equiv 1 \pmod{p}$. Let n be the order of a modulo p. Then $(-a)^{4t+2} \equiv (-1)^{2(2t+1)}a^{4t+2} \equiv 1 \pmod{p}$ so that $4t+2 \mid n$. But $\phi(p) = 4t+2$ so we must have $n = 4t+2$ and a is a primitive root modulo p. □

Problem 10. *Show that the product of all the primitive roots modulo p is congruent to $(-1)^{\phi(p-1)}$ modulo p.*

Proof. Let a be a primitive root modulo p. There are $\phi(p-1)$ primitive roots modulo p and note that every primitive root modulo p can be expressed as some power of a, a^{n_i}. Furthermore we must have $(n_i, p-1) = 1$ otherwise these can't be primitive roots. Note that for every integer n, the sum of all integers t with $1 \le t \le n$ and $(t,n) = 1$ is $\frac{1}{2}n\phi(n)$. Thus the product of all the primitive roots is

$$a^{\sum_{i=1}^{\phi(p-1)} n_i} = a^{\frac{1}{2}(p-1)\phi(p-1)}.$$

But note that $a^{(p-1)/2} \equiv -1 \pmod{p}$ so this reduces to $(-1)^{\phi(p-1)}$ modulo p as desired. □

Problem 11. *Let K be a field and $G \subseteq K^*$ a finite subgroup of the multiplicative group of K. Extend the arguments used in the proof of Theorem 1 to show that G is cyclic.*

Proof. Let $|G| = n$ and for $d \mid n$ define $\psi(d)$ to be the number of elements in G of order d. In any finite commutative group the set of elements x such that $x^d = 1$ form a subgroup. Moreover the order of this subgroup must be at least d. Thus $\sum_{c|d} \psi(c) \le d$. If we apply Möbius inversion we have $\psi(d) \ge \sum_{c|d} \mu(c)d/c = \phi(d)$. In particular $\psi(n) \ge \phi(n)$ which for $n > 1$ is greater than 1. Thus there is at least one element of G which generates the entire group and thus G is cyclic. □