Kris Harper
MATH 24200
May 10, 2010

Homework 4

Problem 1. *Use the Jacobi symbol to determine* $(113/997)$, $(215/761)$, $(514/1093)$, $(401/757)$.

Proof. We see 113 and 997 are both prime. Note $113 \equiv 1 \equiv 5 \pmod 4$ so

$$\begin{aligned}(113/997) = (997/113) = (93/113) = (3/113)(31/113) = (113/3)(113/31) &= (2/3)(20/31)\\ &= (2/3)(2/31)^2(5/31) = (2/3)(5/31)\\ &= (2/3)(31/5) = (2/3)(1/5) = (-1)(1) = -1.\end{aligned}$$

We see 761 is prime. Note also $761 \equiv 1 \equiv 5 \pmod 4$ and $43 \equiv 3 \pmod 4$. Then

$$\begin{aligned}(215/761) = (5/761)(43/761) = (761/5)(761/43) = (1/5)(30/43) &= (2/43)(3/43)(5/43)\\ &= -(-1)^{(43^2-1)/8}(43/3)(43/5)\\ &= (1/3)(3/5) = (1)(-1) = -1.\end{aligned}$$

We see 1093 is prime. Note $1093 \equiv 5 \pmod 8$, $1093 \equiv 1 \equiv 65 \pmod 4$ and $31 \equiv 3 \pmod 4$. Then

$$\begin{aligned}(514/1093) = (2/1093)(257/1093) &= -(1093/257) = -(65/257) = -(257/65)\\ &= -(62/65) = -(65/62) = -(3/62) = -(3/2)(3/31)\\ &= (31/3) = (1/3) = 1.\end{aligned}$$

We see both 401 and 757 are prime. Note also $401 \equiv 1 \equiv 45 \pmod 4$. Then

$$\begin{aligned}(401/757) = (757/401) = (356/401) &= (401/356) = (45/356) = (356/45)\\ &= (41/45) = (45/41)\\ &= (4/41) = (2/41)^2 = 1.\end{aligned}$$

□

Problem 2. *An integer is called a biquadratic residue modulo p if it is congruent to a fourth power. Using the identity $x^4 + 4 = ((x+1)^2+1)((x-1)^2+1)$ show that -4 is a biquadratic residue modulo p iff $p \equiv 1 \pmod 4$.*

Proof. We want to find a solution to the equation $-4 \equiv x^4 \pmod p$ or equivalently $x^4 + 4 \equiv ((x+1)^2 + 1)((x-1)^2+1) \equiv 0 \pmod p$. Note then that this has a solution if and only if one of the factors $((x+1)^2+1)$ or $((x-1)^2+1)$ is congruent to 0 modulo p. Thus we either have $(x+1)^2+1 \equiv 0 \pmod p$ or $(x-1)^2+1 \equiv 0 \pmod p$ In either case -1 is a quadratic residue modulo p which is true if and only $p \equiv 1 \pmod 4$. □

Problem 3. *This exercise and Exercises 27 and 28 give Dirichlet's beautiful proof that 2 is a biquadratic residue modulo p iff p can be written in the form $A^2 + 64B^2$, where $A, B \in \mathbb{Z}$. Suppose that $p \equiv 1 \pmod 4$. Then $p = a^2 + b^2$ by Exercise 24. Take a to be odd. Prove the following statements:*
(a) $(a/p) = 1$.
(b) $((a+b)/p) = (-1)^{((a+b)^2-1)/8}$.
(c) $(a+b)^2 \equiv 2ab \pmod p$.
(d) $(a+b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4} \pmod p$.

Proof. (a) From part (c) and the fact that $p \equiv 1 \pmod 8$ we know $1 = (2ab/p) = (2/p)(a/p)(b/p) = (a/p)(b/p)$ so $(a/p) = (b/p)$. But it's not possible that both a and b are nonresidues modulo p so we must have $(a/p) = 1$.

(b) Note that $2p = (a+b)^2 + (a-b)^2$ and $a+b$ is odd. Thus $(2p/(a+b)) = 1$ since $2 \nmid a+b$. Then $1 = (2/(a+b))(p/(a+b)) = (-1)^{((a+b)^2-1)/8}((a+b)/p)$ since $p \equiv 1 \pmod 4$.

(c) We have $(a+b)^2 \equiv a^2 + 2ab + b^2 \equiv p + 2ab \equiv 2ab \pmod p$.

(d) Since $p \equiv 1 \pmod 4$ we know $k = (p-1)/4$ is an integer. Then from part (c) we have $(a+b)^{2k} \equiv (2ab)^k \pmod p$. Putting in the value of k gives the result. □

Problem 4. *Suppose that f is such that $b \equiv af \pmod p$. Show that $f^2 \equiv -1 \pmod p$ and that $2^{(p-1)/4} \equiv f^{ab/2} \pmod p$.*

Proof. Note that $b^2 \equiv a^2 f^2 \pmod p$ and that $0 \equiv a^2 + b^2 \equiv a^2 + a^2 f^2 = a^2(1+f^2)$. Since a^2 is not equivalent to 0 modulo p we see that $0 \equiv 1 + f^2 \pmod p$ and $f^2 \equiv -1 \pmod p$. Raising this to the power $ab/2$ and using Problem 3 gives the second result. □

Problem 5. *Show that $x^4 \equiv 2 \pmod p$ has a solution for $p \equiv 1 \pmod 4$ iff p is of the form $A^2 + 64B^2$.*

Proof. If $p = A^2 + 64B^2$ then let $a = A$ and $b = 8B$ so that $p = a^2 + b^2$. Then using Problem 4 we know there exists f such that $f^{ab/2} \equiv 2^{(p-1)/2} \pmod p$. Since $4 \mid ab/2$ we see that $x^4 \equiv 2 \pmod p$ is solvable. Conversely, suppose that $x^4 \equiv 2 \pmod p$ is solvable. Since $p \equiv 1 \pmod 4$ we know $p = a^2 + b^2$ and we only need to show that $8 \mid b$. But this must be the case since Problem 4 tells us that $2^{(p-1)/4} \equiv f^{ab/2} \pmod p$ and $2 \equiv x^4 \pmod p$ for some x. Raising 2 the the power $(p-1)/4$ shows that $4 \mid ab/2$. Since a is odd we must have $8 \mid b$. □

Problem 6. *Show that $\sqrt{2} + \sqrt{3}$ is an algebraic integer.*

Proof. Note that $\sqrt{2}$ is a root to $x^2 - 2$ and $\sqrt{3}$ is a root to $x^2 - 3$. These are both monic polynomials with coefficients in $\mathbb{Z}$, so $\sqrt{2}$ and $\sqrt{3}$ are both algebraic integers. Since the algebraic integers form a ring, it follows that $\sqrt{2} + \sqrt{3}$ is also an algebraic integer. □

Problem 7. *Let α be an algebraic number. Show that there is an integer n such that $n\alpha$ is an algebraic integer.*

Proof. Since α is algebraic there exists some polynomial $p(x) \in \mathbb{Q}[x]$ such that $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$ and $a_i \in \mathbb{Q}$. Now find the least common multiple of the a_i and call it n. Multiply our polynomial by n so we have $n\alpha^m + b_1\alpha^{m-1} + \cdots + b_m = 0$ where $b_i \in \mathbb{Z}$. Finally, multiply both sides by n^{m-1} so we have $n^m\alpha^m + b_1 n^{m-1}\alpha^{m-1} + b_2 n^{m-1}\alpha^{m-2} + \cdots + b_m n^{m-1} = 0$. We can now pass the appropriate exponent of n inside each exponent of α for every term which results in the equation $(n\alpha)^m + b_1(n\alpha)^{m-1} + b_2 n(n\alpha)^{m-2} + \cdots + b_{m-1}n^{m-2}(n\alpha) + b_m n^{m-1} = 0$. Since each $b_i n^{i-1}$ is an integer we see that $n\alpha$ is an algebraic integer. □

Problem 8. *If α and β are algebraic integers, prove that any solution to $x^2 + \alpha x + \beta = 0$ is an algebraic integer. Generalize this result.*

Proof. Since α and β are algebraic integers they satisfy polynomials in $\mathbb{Z}[x]$ of the form $\alpha^n + a_{n-1}\alpha^{n-1} \cdots + a_0 = 0$ and $\beta^m + b_{m-1}\beta^{m-1} + \cdots + b_0 = 0$. Let γ be a root of $x^2 + \alpha x + \beta$ and let V be the $\mathbb{Z}$ module generated by $\alpha^i\beta^j\gamma^k$ where $0 \le i \le n$, $0 \le j \le m$ and $0 \le k \le 1$. Then consider $\gamma\alpha^i\beta^j\gamma^k$. If $k = 0$ then this is clearly in V. If $k = 1$ then $\gamma\alpha^i\beta^j\gamma^k = \alpha^i\beta^j\gamma^2 = \alpha^i\beta^j(-\alpha\gamma - \beta) = -\alpha^{i+1}\beta^j\gamma^k - \alpha^i\beta^{j+1}$. This is also definitely an element of V except for the possibility that $i = n$ or $j = m$. In this case we simply rewrite $\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_0)$ and $\beta^m = -(b_{m-1}\beta^{m-1} + \cdots + b_0)$. Expanding this out gives an element of V. This statement generalizes so that if γ is a root of $x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0$ where the α_i are algebraic integers then γ is an algebraic integer. □

Problem 9. *Let $\omega = e^{2\pi i/3}$. ω satisfies $x^3 - 1 = 0$. Show that $(2\omega + 1)^2 = -3$ and use this to determine $(-3/p)$ by the method of section 2.*

Proof. We have $(2\omega+1)^2 = 4\omega^2+4\omega+1 = 4(\omega^2+\omega+1)-3 = -3$. Note that if $p = 3$ then $(-3/p) = 0$ so we can assume $p \neq 3$. Let $\tau = 2\omega+1$. Then $\tau^{p-1} = (\tau^2)^{(p-1)/2} = (-3)^{(p-1)/2} \equiv (-3/p) \pmod{p}$ and $\tau^p \equiv (-3/p)\tau \pmod{p}$. Note $\tau^p = (2\omega+1)^p \equiv 2^p\omega^p + 1 \pmod{p}$. Since $\omega^3 = 1$ we have $2^p\omega^p + 1 \equiv 2^p\omega + 1 \equiv 2\omega + 1 \equiv \tau \pmod{p}$ if $p \equiv 1 \pmod{3}$ and $2^p\omega^p \equiv 2^p\omega^2 + 1 \equiv 2(-\omega-1)+1 \equiv -2\omega - 1 \equiv -\tau \pmod{p}$ if $p \equiv 2 \pmod{3}$. We can now express this as $(-1)^\varepsilon\tau \equiv (-3/p)\tau \pmod{\tau}$ where $\varepsilon = 3((p/3) - \lfloor (p/3) \rfloor) - 1$. Multiply both sides by τ and note that we can divide by -3 to get $(-3/p) = (-1)^\varepsilon$. □

Problem 10. *By calculating* $\sum_t (1 + (t/p))\zeta^t$ *in two ways prove that* $g = \sum_t \zeta^{t^2}$.

Proof. Note that

$$g = \sum_t \left(\frac{t}{p}\right)\zeta^t = \sum_t \zeta^t + \sum_t \left(\frac{t}{p}\right)\zeta^t = \sum_t \left(1 + \left(\frac{t}{p}\right)\right)\zeta^t = \sum_t \zeta^{t^2}$$

since $1 + (t/p)$ is the number of solutions to $x^2 \equiv t \pmod{p}$. □