

567 Number Theory I, Fall Term 2008, Solutions 14

1. (i) Prove that if $p \equiv 1 \pmod{3}$, then $\left(\frac{-3}{p}\right)_L = 1$. By quad. recip. $\left(\frac{-3}{p}\right)_L = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)_L = 1$.

(ii) Let $\mathcal{M} = \{n \in \mathbb{N} : p|n \implies p \equiv 1 \pmod{3}\}$. Prove that if $n \in \mathcal{M}$, then $x^2 + 3 \equiv 0 \pmod{4n}$ is soluble in x . By (i), $x^2 + 3 \equiv 0 \pmod{p}$ is soluble when $p \equiv 1 \pmod{3}$, and $1^2 + 3 \equiv 0 \pmod{4}$. Moreover a residue modulo p^k is a quadratic residue iff it is one modulo p . Conclusion follows by Chinese remainder theorem.

(iii) Let $n \in \mathcal{M}$. Prove that there are $a, B \in \mathbb{Z}$ with $a > 0$ such that $B^2 + 12 = 4an$. Let $b = B - 2a$, $c = (b^2 + 12)/4a$. Prove that $b^2 - 4ac = -12$ and $a + b + c = n$. By (ii), $x^2 + 3 \equiv 0 \pmod{n}$ is soluble. Hence there is a solution with $x > n$. Let $a = (x^2 + 3)/n$. Then $B = 2x$ satisfies $B^2 + 12 = 4an$. Moreover $b^2 - 4ac = -12$ and $a + b + c = a + b + \frac{b^2+12}{4a} = a + B - 2a + \frac{B^2-4Ba+4a^2+12}{4a} = n$.

(iv) Let $h(d)$ be defined as in homework 11. Prove that $h(-12) = 2$. Consider $b^2 - 4ac = -12$ with $-a < b \leq a < c$ or $0 \leq b \leq a = c$. In either case b is even and $a^2 - 4a^2 \geq -12$, so $a^2 \leq 4$, $a = 1$ or 2 . When $a = 1$, since b is even, $b = 0$ and so $c = 3$ is the only solutions. When $a = 2$, $8 \nmid 12$ so $b \neq 0$. Hence $b = c = 2$ is the only solution.

(v) Prove that if $n \in \mathcal{M}$, then $x^2 + 3y^2 = n$ is soluble in integers x and y . By (iii), when $n \in \mathcal{M}$, n is represented by $ax^2 + bxy + cy^2$ where $b^2 - 4ac = -12$ and so is represented by at least one of the reduced forms. But n is odd, so it is represented by $x^2 + 3y^2$.

2. (i) Prove that if $p \equiv 1, 4 \pmod{7}$, then $\left(\frac{-7}{p}\right)_L = 1$. By the law of quad. recip.

$$\left(\frac{-7}{p}\right)_L = \left(\frac{7}{p}\right)_L = \left(\frac{p}{7}\right)_L = 1.$$

(ii) Let $\mathcal{N} = \{n \in \mathbb{N} : p|n \implies p \equiv 1, 4 \pmod{7}\}$. Prove that if $n \in \mathcal{N}$, then $x^2 + 7 \equiv 0 \pmod{4n}$ is soluble in x . $1^2 + 7 \equiv 0 \pmod{4}$. Moreover a residue modulo p^k is a quadratic residue iff it is one modulo p . Hence, by (i) and the Chinese remainder theorem $x^2 + 7 \equiv 0 \pmod{4n}$

(iii) Let $n \in \mathcal{N}$. Prove that there are $a, B \in \mathbb{Z}$ with $a > 0$ such that $B^2 + 7 = 4an$. Let $b = B - 2a$, $c = (b^2 + 7)/4a$. Prove that $b^2 - 4ac = -7$ and $a + b + c = n$. By

(ii) there are $B > n$ such that $B^2 + 7 \equiv 0 \pmod{4n}$. Let $a = (B^2 + 7)/4n$. Then $b^2 - 4ac = -7$ and $a + b + c = a + b + \frac{b^2+7}{4a} = a + B - 2a + \frac{B^2-4Ba+a^2+7}{4a} = \frac{B^2+7}{4a} = n$.

(iv) Recall from homework 11 that $h(-7) = 1$. Prove that if $n \in \mathcal{N}$, then $x^2 + xy + 2y^2 = n$ is soluble in integers x and y . By (iii), n is represented by $ax^2 + bxy + cy^2$ with $b^2 - 4ac = -7$. Hence it is represented by the lone reduced form $x^2 + xy + 2y^2$ with discriminant -7 .

(v) Let $n \in \mathcal{N}$. Prove that $x^2 + 7y^2 = 4n$ is soluble in integers x, y . Moreover prove that x and y are both even, and thus $x^2 + 7y^2 = n$ is also soluble in integers x, y . By (iv), $x^2 + xy + 2y^2 = n$. Hence $4n = (2x + y)^2 + 7y^2$, so $4n$ has a representation $4n = x^2 + 7y^2$. Either x and y are both odd or both even. But if they are both odd, then $x^2 + 7y^2 \equiv 1 + 7 \equiv 0 \pmod{8}$ and $8 \nmid n$.