

MATH 567 FALL 2008, NUMBER THEORY I, SOLUTIONS 8

1. Evaluate  $\left(\frac{313}{367}\right)_J$ ,  $\left(\frac{367}{401}\right)_J$ ,  $\left(\frac{401}{313}\right)_J$ .  $313 \equiv 401 \equiv 1 \pmod{8}$ ,  $367 \equiv 7 \pmod{8}$ . Thus  $(313|367)_J = (367|313)_J = (6|313)_J = (2|313)_J(3|313)_J = (313|3)_J = 1$ ,  $(367|401)_J = (401|367)_J = (2|367)_J(17|367)_J = (367|17)_J = (10|17)_J = (5|17)_J = (2|5)_J = -1$ ,  $(401|313)_J = (88|313)_J = (11|313)_J = (5|11)_J = (1|5)_J = 1$ .
2. Show that the congruence  $x^6 - 11x^4 + 36x^2 - 36 \equiv 0 \pmod{p}$  is soluble for every prime  $p$ .  $x^6 - 11x^4 + 36x^2 - 36 = (x^2 - 2)(x^2 - 3)(x^2 - 6)$ . If 2 or 3 is a QR we are done. If not, then 6 is a QR.
3. Suppose that  $a \in \mathbb{Z} \setminus \{0\}$ , and there is a  $b \in \mathbb{Z}$  such that  $a = -b^2$ . Show that there is an odd positive integer  $m$  such that  $\left(\frac{a}{m}\right)_J = -1$ . Deduce that there is an odd prime  $p$  such that  $\left(\frac{a}{p}\right)_J = -1$ . Choose  $m \equiv -1 \pmod{4b}$ . Then  $(-b^2|m)_J = -(b|m)_J^2 = -1$ . Moreover not all the primes  $p$  with  $p|m$  can satisfy  $(-b^2|p)_L = 1$ .
4. Suppose that  $a \in \mathbb{Z} \setminus \{0\}$  and  $a = \pm 2^u b$  where  $u \in \mathbb{N}$  and  $b \in \mathbb{N}$  with both  $u$  and  $b$  odd. Show that there is an odd positive integer  $m$  such that  $\left(\frac{a}{m}\right)_J = -1$ . Deduce that there is an odd prime  $p$  such that  $\left(\frac{a}{p}\right)_J = -1$ . Choose  $m$  so that  $m \equiv 5 \pmod{8}$  and  $m \equiv 1 \pmod{b}$ . Then  $(\pm 2^u b|m)_J = (2|m)_J(b|m)_J = -(m|b)_J = -1$ . Moreover not all the primes  $p$  with  $p|m$  can satisfy  $(\pm 2^u b|m|p)_L = 1$ .
5. Suppose that  $a \in \mathbb{Z} \setminus \{0\}$  and  $a = \pm 2^{2u} b q^t$  where  $u$  is a non-negative integer,  $b \in \mathbb{N}$  and  $t \in \mathbb{N}$  with both  $b$  and  $t$  odd, and  $q$  is an odd prime with  $q \nmid b$ . Show that there is an odd positive integer  $m$  such that  $\left(\frac{a}{m}\right)_J = -1$ . Deduce that there is an odd prime  $p$  such that  $\left(\frac{a}{p}\right)_J = -1$ . Choose  $m$  so that  $m \equiv 1 \pmod{4b}$  and  $m$  is a QR  $n \pmod{q}$ . Then  $(\pm 2^{2u} b q^t|m)_J = (m|b)_J(m|q)_L = -1$ . Moreover not all the primes  $p$  with  $p|m$  can satisfy  $(\pm 2^{2u} b q^t|p)_L = 1$ .
6. Show that an integer  $a$  is a perfect square if and only if it is a quadratic residue for every prime  $p$  not dividing  $a$ . If  $a$  is a perfect square then at once it is a QR modulo  $p$  for every such  $p$ . If  $a$  is not a perfect square, then it is of one of the forms  $-b^2$ ,  $\pm 2^u b$  where  $u \in \mathbb{N}$  and  $b \in \mathbb{N}$  with both  $u$  and  $b$  odd, or  $\pm 2^{2u} b q^t$  where  $u$  is a non-negative integer,  $b \in \mathbb{N}$  and  $t \in \mathbb{N}$  with both  $b$  and  $t$  odd, and  $q$  is an odd prime with  $q \nmid b$ . Hence by questions 3, 4 or 5, there is always an odd prime  $p$  such that  $a$  is a QNR modulo  $p$ .