SOLUTIONS TO HOMEWORK 8

1. Use quadratic reciprocity:

$$\left(\frac{264}{173}\right) = \left(\frac{2}{173}\right)^3 \left(\frac{33}{173}\right) = (-1)^{(33-1)(173-1)/4} \left(\frac{2}{173}\right)\left(\frac{173}{33}\right)$$
$$= (-1)^{(173^2-1)/8} \left(\frac{8}{173}\right) = -\left(\frac{2}{33}\right) = -(-1)^{(33^2-1)/8} = -1,$$

and

$$\left(\frac{2019}{4987}\right) = (-1)^{(4987-1)(2019-1)/4} \left(\frac{4987}{2019}\right) = -\left(\frac{4987}{2019}\right) = -\left(\frac{949}{2019}\right)$$
$$= -(-1)^{(2019-1)(949-1)/4} \left(\frac{2019}{949}\right) = -\left(\frac{121}{949}\right) = -\left(\frac{11}{949}\right)^2 = -1,$$

and

$$\left(\frac{187}{389}\right) = (-1)^{(187-1)(389-1)/4} \left(\frac{389}{187}\right) = \left(\frac{15}{187}\right) = (-1)^{(15-1)(187-1)/4} \left(\frac{187}{15}\right)$$
$$= -\left(\frac{7}{15}\right) = -\left(\frac{-8}{15}\right) = -(-1)^{(15-1)/2} \left(\frac{2}{15}\right)^3 = \left(\frac{2}{15}\right)$$
$$= (-1)^{(15^2-1)/8} = 1.$$

2. (a) By quadratic reciprocity, one has

$$\left(\frac{5}{p}\right) = (-1)^{(5-1)(p-1)/4} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right).$$

But $1^2 \equiv 4^2 \equiv 1 \pmod 5$ and $2^2 \equiv 3^2 \equiv 4 \pmod 5$. Then we deduce that $\left(\frac{p}{5}\right) = 1$ if and only if $p \equiv 1, 4 \pmod 5$. Thus we conclude that 5 is a quadratic residue modulo p if and only if $p \equiv 1$ or 4 modulo 5.

(b) Suppose that there are only finitely many primes p of the shape $5k + 4$, say $p_1, \ldots, p_n$. Note that 19 is one such prime. Put $Q = (2p_1 \ldots p_n)^2 - 5$. The first part of this question shows that the only odd prime divisors p of Q must have the shape either $5k + 1$ or $5k + 4$. But since $p_i^2 \equiv 4^2 \equiv 1 \pmod 5$, we have $Q \equiv 4 \pmod 5$, so that the odd number Q must have at least one prime divisor of the shape $5k+4$. Moreover, for each i one has $(Q, p_i) = (-5, p_i) = 1$, so that $p_i \nmid Q$. Thus we deduce that Q is divisible by some prime of the shape $5k+4$ not amongst $p_1, \ldots, p_n$, yielding a contradiction. We conclude that there are infinitely many primes of the shape $5k + 4$.

3. By quadratic reciprocity, one has

$$\left(\frac{-7}{p}\right) = (-1)^{(p-1)/2} \left(\frac{7}{p}\right) = (-1)^{(p-1)/2+(7-1)(p-1)/4} \left(\frac{p}{7}\right) = \left(\frac{p}{7}\right).$$

But $1^2 \equiv 6^2 \equiv 1 \pmod 7$, $2^2 \equiv 5^2 \equiv 4 \pmod 7$, and $3^2 \equiv 4^2 \equiv 2 \pmod 7$. Then we deduce that $\left(\frac{p}{7}\right) = 1$ if and only if $p \equiv 1, 2, 4 \pmod 7$. Thus we conclude that -7 is a quadratic residue modulo p if and only if $p \equiv 1, 2, 4 \pmod 7$.

4. (a) When $p \equiv 5 \pmod{12}$, it follows from quadratic reciprocity thatone has

$$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

(b) When $p = 2^{2^n} + 1$ is prime, it follows from Fermat's Little Theorem that the order of 3 modulo p divides $p - 1 = 2^{2^n}$. Then the order of 3 modulo p is a power of 2, and if 3 is not a primitive root, then this order divides $2^{2^n - 1} = (p-1)/2$. In such circumstances, we find from part (a) via Euler's criterion that

$$-1 = \left(\frac{3}{p}\right) \equiv 3^{(p-1)/2} \equiv 1 \pmod p,$$

yielding a contradiction. Thus 3 must be a primitive root modulo p.

5. (a) Suppose that x and y are integers with $y^2 = x^3 + 45$. Observe that $y^2 \equiv 0$, 1 or 4 modulo 8. If $y^2 \equiv 1 \pmod 8$, then $x^3 \equiv 4 \pmod 8$, which is impossible. If $y^2 \equiv 0 \pmod 8$, then $x^3 \equiv 3 \pmod 8$, whence $x \equiv 3 \pmod 8$. If $y^2 \equiv 4 \pmod 8$, then $x^3 \equiv 7 \pmod 8$, whence $x \equiv 7 \pmod 8$. Thus we deduce that $x \equiv 7 \pmod 8$ or $x \equiv 3 \pmod 8$.

(b) If $x \equiv 7 \pmod 8$, then $x^2 - 3x + 9 \equiv 5 \pmod 8$, and so it is impossible that $x^2 - 3x + 9$ is divisible only by primes congruent to ± 1 modulo 8. Consequently, $x^2 - 3x + 9$ must be divisible by a prime congruent to $\pm 3 \pmod 8$. Given such a prime p, since $y^2 - 2 \cdot 3^2 = (x+3)(x^2 - 3x + 9)$, one must have $y^2 \equiv 2 \cdot 3^2 \pmod p$, whence $p = 3$ or $\left(\frac{2}{p}\right) = 1$. But the latter is possible if and only if $p \equiv \pm 1 \pmod 8$, and this yields a contradiction. Thus we find that $p = 3$ and $3|y$, and the equation $y^2 = x^3 + 45$ then implies that $3|x$ and hence $(y/3)^2 \equiv 2 \pmod 3$, again yielding a contradiction.

(c) When $x \equiv 3 \pmod 8$, one has $x^2 + 3x + 9 \equiv 3 \pmod 8$, and moreover it is impossible that $x^2 + 3x + 9$ is divisible only by primes congruent to ± 1 modulo 8. Then $x^2 + 3x + 9$ is divisible by a prime $p \equiv \pm 3 \pmod 8$, whence $y^2 \equiv 2 \cdot 6^2 \pmod p$. Thus $p = 3$ or $\left(\frac{2}{p}\right) = 1$. The former is impossible just as in (b), and the latter is again possible if and only if $p \equiv \pm 1 \pmod 8$. We therefore again arrive at a contradiction.

We may consequently conclude that the equation $y^2 = x^3 + 45$ is insoluble in integers x and y.