Solutions to Sheet 7

1(a)

Let $n-1 = 2^s t$ and consider the quantities $b^{2^s t} \mod n, b^{2^{s-1}t} \mod n, \ldots, b^{2t} \mod n, b^t \mod n$. Since n is prime, by Fermat's little theorem $b^{n-1} \equiv 1(\mod n)$. Further since n is prime, $x^2 \equiv 1(\mod n)$ implies either $x \equiv 1(\mod n)$ or $x \equiv -1(\mod n)$. This implies that the qunatiities considered above are either all 1 or we have a sequence of 1's followed by a -1. In the former case we have $b^t \equiv 1(\mod n)$ while in the latter we have a $j, 0 \leq j \leq s-1$, such that $b^{2^j t} \equiv -1(\mod n)$. Thus n passes the Miller test.

1(b)

Note that $2047 = 23 \times 89$ and is hence composite. Further $2046 = 2 \times 1023$ and so to show that 2047 pases the miller test it suffices to show that $2^{1023} \equiv 1(\mod 2047)$. Note that $2^{11} = 2048 \equiv 1(\mod 2047)$. Hence $2^{1023} = 2^{11\times 93} \equiv 1^{93} \equiv 1(\mod 2047)$.

2(a)

Note that $1729 = 7 \times 13 \times 19$ and $1728 = 2^6 \times 3^3$. Consider an a, such that $\gcd(a, 1729) = 1$. This implies a is coprime with 7, 13, 19 and hence by Fermat's little theorem $a^6 \equiv 1(\mod 7), a^{12} \equiv 1(\mod 13), a^{18} \equiv 1(\mod 19)$. Since 6, 12 and 18 divide 1728 we get that $a^{1728} = a^{6\times 288} \equiv 1(\mod 7)$, $a^{1728} = a^{12\times 144} \equiv 1(\mod 13)$, $a^{1728} = a^{18\times 96} \equiv 1(\mod 19)$. Since 7, 13 and 19 are relatively prime, by Chinese remainder theorem we obtain that $a^{1728} \equiv 1(\mod 1729)$ which implies 1729 is Carmichael.

2(b)

Note that $2821 = 7 \times 13 \times 31$ and $2820 = 2^2 \times 3 \times 5 \times 47$. Consider an a, such that $\gcd(a, 2821) = 1$. This implies a is coprime with 7, 13, 31 and hence by Fermat's little theorem $a^6 \equiv 1(\mod 7), a^{12} \equiv 1(\mod 13), a^{30} \equiv 1(\mod 31)$. Since 6, 12 and 30 divide 2820 we get that $a^{2820} = a^{6\times 470} \equiv 1(\mod 7)$, $a^{2820} = a^{12\times 235} \equiv 1(\mod 13)$, $a^{2820} = a^{30\times 94} \equiv 1(\mod 31)$. Since 7, 13 and 31 are relatively prime, by Chinese remainder theorem we obtain that $a^{2820} \equiv 1(\mod 2821)$ which implies 2821 is Carmichael.

2(c)

Consider an a, such that $\gcd(a, n) = 1$. This implies a is coprime with $p_1, p_2, ..., p_k$ and hence by Fermat's little theorem $a^{p_i - 1} \equiv 1(\mod p_i)$, $1 \leq i \leq k$. Since $p_i - 1 | n-1$ for $i = 1, 2, ..., k$, we get that $a^{n-1} = a^{(p_i-1)\times(n-1)/(p_i-1)} \equiv 1(\mod p_i)$. Since $p_1, p_2, ..., p_k$ are relatively prime, by Chinese remainder theorem we obtain that $a^{n-1} \equiv 1(\mod n)$ which implies n is Carmichael.

3(a)

a is a quadratic residue of 11 iff $\exists i$, $1 \leq i \leq 10$, $i^2 \equiv a(\mod 11)$. We compute $i^2 \mod 11$ for $1 \leq i \leq 10$, and get the multiset $\{1, 4, 9, 5, 3, 3, 5, 9, 4, 1\}$. Thus $\{1, 3, 4, 5, 9\}$ are quadratic resideues of 11.

3(b)

Note that if r is a solution to $x^2 \equiv a(\mod p)$ then so is $(p-r)$ since $r^2 \equiv (p-r)^2 \mod p$. Since p is odd, $r \neq p-r$. Let s be a third solution i.e. $s \not\equiv r(\mod p)$ and $s \not\equiv -r(\mod p)$. Then $r^2 \equiv s^2(\mod p)$ and hence $p | (r-s)(r+s)$. Since p is prime, either $p|(r-s)$ or $p|(r+s)$ which implies either $r \equiv s(\mod p)$ or $s \equiv -r(\mod p)$. Hence, no third solution is possible and the congruence has either no solution or exactly two incongruent solutions modulo p.

3(c)

Consider the $(p-1)/2$ pairs $(i, p-i)$ for $1 \leq i \leq (p-1)/2$. From 3(b) we have seen that, $i^2 \equiv (p-i)^2(\mod p) = a_i$(say). Further (again from 3(b)), if $i \neq j$ then $a_i \neq a_j$. Hence $a_1, a_2, \ldots, a_{(p-1)/2}$ are $(p-1)/2$ distinct numbers between 1 and $p-1$ that are quadratic residues of p.

4(a)

We need to show that if $a \equiv b(\mod p)$, then a is a quadratic residue of p iff b is a quadratic residue of p. If a is a quadratic residue than $x^2 \equiv a(\mod p)$ has a solution, say r. But then $r^2 \equiv a \equiv b(\mod p)$ and so b is also a quadratic residue.

4(b)

If a is a quadratic residue of p then $\exists r, r^2 \equiv a(\mod p)$. Since a is not a multiple of p, neither is r. Hence by Fermat's little theorem, $r^{p-1} \equiv a^{(p-1)/2} \equiv 1(\mod p)$ and hence $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(\mod p)$.

If a is not a quadratic residue then we consider the set $S = \{1, 2, 3, \ldots, p-1\}$.

1. The product of the elements of S is $(p-1)!$ which by Wilson's theorem is equivalent to $-1(\mod p)$.

2. Next we pair the elements of S with i, j forming a pair iff $i \cdot j \equiv a(\mod p)$.

   (a) This pairing is well defined since if $i \cdot j \equiv a \equiv i \cdot k(\mod p)$ then $i^{-1} \cdot i \cdot j \equiv i^{-1} \cdot i \cdot k(\mod p)$. Hence $j \equiv k(\mod p)$ which, since $1 \leq j, k \leq p-1$, implies $j = k$.

   (b) Further if $i \cdot j \equiv a(\mod m)$ then, since a is not a quadratic residue, we have $i \neq j$.

3. The pairing implies that the product of the elements in S is $a^{(p-1)/2}(\mod p)$.

From (1) and (3) we conclude that when a is not a quadratic residue $a^{(p-1)/2} \equiv -1(\mod p)$ and hence $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(\mod p)$.

4(c)

Note that modulo p, $\left(\frac{ab}{p}\right) = (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

5

In 4(b) we proved that -1 is a quadratic residue of p iff $(-1)^{(p-1)/2} \equiv 1(\mod p)$. When $p = 4k+1$, then $(p-1)/2 = 2k$ and hence $(-1)^{(p-1)/2} = 1$. Similarly -1 is a quadratic non-residue iff $(-1)^{(p-1)/2} \equiv -1(\mod p)$. When $p = 4k+3$, then $(p-1)/2 = 2k+1$ and hence $(-1)^{(p-1)/2} = -1$.

6

We consider the conguences $x^2 \equiv 29 \equiv 4(\mod 5)$ and $x^2 \equiv 29 \equiv 1(\mod 7)$. By the Chinesese remainder theorem, any solution to this system of congruences also satisfies the original congruence. Solutions to the first congruence satisfy $x \equiv 2(\mod 5)$ or $x \equiv -2(\mod 5)$. Similarly, solutions to the second congruence satisfy $x \equiv 1(\mod 7)$ or $x \equiv -1(\mod 7)$. This yields 4 different system of congruences:

1. $x \equiv 2(\mod 5)$ and $x \equiv 1(\mod 7)$ which has the solution x=22.
2. $x \equiv 2(\mod 5)$ and $x \equiv -1(\mod 7)$ which has the solution x=27.
3. $x \equiv -2(\mod 5)$ and $x \equiv 1(\mod 7)$ which has the solution x=8.
4. $x \equiv -2(\mod 5)$ and $x \equiv -1(\mod 7)$ which has the solution x=13.

Hence the congruence $x^2 \equiv 29(\mod 35)$ has solutions $\{8, 13, 22, 27\}$