18.781 Homework 6

Due: 18th March 2014

Q 1 (2.8(24)). Let $a$ and $n > 1$ be any integers such that $a^{n-1} \equiv 1 \pmod{n}$ but $a^d \not\equiv 1 \pmod{n}$ for every proper divisor $d$ of $n - 1$. Prove that $n$ is a prime.

Proof. Suppose $n$ is not prime. We consider two cases, first where $n$ has at least two prime factors and the second where $n$ is a prime power and draw a contradiction in either case. First assume $n$ has at least two prime factors. They we may write $n = kl$ for some positive integers $k > 1$ and $l > 1$ and $(k, l) = 1$. For any $a$ coprime to $n$, we have $(a, k) = 1$ and $(a, l) = 1$ and that $a^{\varphi(k)} \equiv 1 \pmod{k}$ and $a^{\varphi(l)} \equiv 1 \pmod{l}$ by Euler’s congruence. This tells us that $a^{\varphi(k)\varphi(l)} \equiv 1 \pmod{k}$ and $a^{\varphi(k)\varphi(l)} \equiv 1 \pmod{l}$. As $(k, l) = 1$, this tells us that $a^{\varphi(k)\varphi(l)} \equiv 1 \pmod{kl}$. The statement says that there is an element of order $n - 1$ modulo $n$. This tells us that $n - 1 \mid \varphi(k)\varphi(l)$. $\varphi(k)\varphi(l) \neq 0$ and $\varphi(k) \leq k - 1$ and $\varphi(l) \leq l - 1$. This tells us that $\varphi(k)\varphi(l) \leq (k - 1)(l - 1) = n - (k + l - 1) < n - 1$ as $k > 1$ and $l > 1$. This is a contradiction. If $n = p^r$ for some prime $p$ and positive integer $r > 1$, then for any integer $a$, $a^{p^r-1(p-1)} \equiv 1 \pmod{n}$ and if there is an element of order $n - 1$ modulo $n$, then we must have $n - 1 \mid p^{r-1}(p-1)$ which is impossible.

Q 2 (2.8(33)). Let $k$ and $a$ be positive integers, with $a \geq 2$. Show that $k \mid \varphi(a^k - 1)$.

Proof. It suffices to show that there is an element $b$, coprime to $a^k - 1$, of order $k$ modulo $a^k - 1$ by Corollary 2.32. We claim $b = a$ does the job. Clearly $(a, a^k - 1) = 1$ and $a^k \equiv 1 \pmod{a^k - 1}$. If $a$ has order $h$ modulo $a^k - 1$, then $h \mid k$, so $1 \leq h \leq k$. If $h < k$, then $a - 1 \leq a^h - 1 < a^k - 1$, so $a^k - 1 \not\equiv a^h - 1$. This proves $h = k$.

Q 3 (2.8(34)). Show that if $p \mid \varphi(m)$ and $p \nmid m$ then there is at least one prime factor $q$ of $m$ such that $q \equiv 1 \pmod{m}$.

Proof. Write $m = \prod q_i^{r_i}$ for some primes $q_i$ and integers $r_i \geq 1$. $p \nmid m$ is equivalent to $(p, m) = 1$ which is equivalent to $(p, q_i) = 1$ for every $i$. This in turns implies $(p, \prod q_i^{(r_i-1)}) = 1$ or equivalently $p \nmid \prod q_i^{(r_i-1)}$. $\varphi(m) = \prod q_i^{(r_i-1)}\prod(q_i - 1)$. As $p$ is prime and $p \mid \varphi(m)$, this implies $p \mid q_i - 1$ for some $i$ or equivalently $q_i \equiv 1 \pmod{m}$ for some $i$.

Q 4 (2.8(35)). Let $p$ be a given prime number. Prove that there exist infinitely many prime numbers $q \equiv 1 \pmod{m}$.

Proof. Suppose there were only finitely many primes $q$ such that $q \equiv 1 \pmod{p}$. List them as $\{q_1, q_2, \ldots, q_r\}$. Let $a = p\prod_{i=1}^r q_i$ and $k = p$. Then $a \geq p \geq 2$. Then by Problem 33, we have that $p \mid \varphi(a^k - 1)$, but $p \mid a^k$, so $a^k - 1 \equiv -1 \pmod{m} \neq 0 \pmod{m}$. So we may now apply Problem 34 to conclude that there is a prime factor $q$ of $a^k - 1$ such that $q \equiv 1 \pmod{p}$. This implies $q = q_i$ for some $i$. But $q_i \mid a$, so $q_i \mid a^{k-1}$ for $1 \leq i \leq r$, so this is a contradiction.

Q 5 (2.8(36)(i)-(vii)). Primes $\equiv 1 \pmod{m}$. For any positive integer $m$, prove that the arithmetic progression

$$1 + m, 1 + 2m, 1 + 3m, \ldots, (\ast m)$$

contains infinitely many primes. An elementary proof of this is outlined in parts (i) to (vii) below. (The argument follows that of J.Niven and B. Powell, "Primes in certain arithmetic progressions," Amer. Math. Monthly, 83 (1976), 467-469, as simplified by R. W. Johnson.)
(i) Prove that it suffices to show that for every positive integer \( m \), the arithmetic progression \((\ast m)\) contains at least one prime. Note also that we may suppose that \( m \geq 3 \).

We now show that for any integer \( m \geq 3 \), the number \( m^{m-1} - 1 \) has at least one prime divisor \( \equiv 1 \pmod{m} \).

We suppose that \( m \geq 3 \) and that \( m^{m-1} - 1 \) has no prime divisor \( \equiv 1 \pmod{m} \), and derive a contradiction.

(ii) Let \( q \) be any prime divisor of \( m^{m-1} - 1 \), so that \( q \nmid 1 \pmod{m} \). Let \( h \) denote the order of \( m \pmod{q} \), so that \( m^h \equiv 1 \pmod{q} \), and moreover \( m^d \equiv 1 \pmod{m} \) if and only if \( h \mid d \), by Lemma 2.31. Verify that \( h \mid (q - 1) \) and \( h \mid m \). Prove that \( h < m \), so that \( m = hc \) with \( c > 1 \).

(iii) Let \( q^r \) be the highest power of \( q \) dividing \( m^d - 1 \); thus \( q^r \mid (m^d - 1) \). Prove that \( q^r \mid (m^b - 1) \), and that \( q^r \mid (m^d - 1) \) for every integer \( d \) such that \( h \mid d \) and \( d \mid m \).

These properties of \( q \) hold for any prime divisor of \( m^{m-1} - 1 \). Of course different prime factors may give different values of \( h \), \( c \), and \( r \), because these depend on \( q \). To finish the proof we need one additional concept. Consider the set of integers of the form \( m/s \), where \( s \) is any square-free divisor of \( m \), excluding \( s = 1 \). We partition this set into two disjoint subsets \( T \) and \( V \) according as the number of primes dividing \( s \) is odd or even. Put

\[
Q = \left( \prod_{d \in T} (m^d - 1) \right) \left( \prod_{d \in V} (m^d - 1) \right)^{-1}.
\]

(iv) Let \( q \) be the prime factor of \( m^{m-1} - 1 \) under consideration, and let \( m^d - 1 \) be a factor that occurs in one of the two products displayed. Use (ii) to show that \( q \mid (m^d - 1) \) if and only if \( s \mid c \).

(v) Let \( k \) denote the number of distinct primes dividing \( c \). Show that the number of \( d \in T \) for which \( q \mid (m^d - 1) \) is \( \frac{k}{1} + \frac{k}{2} + \frac{k}{3} + \cdots \) and that this sum is \( 2^k - 1 \). Similarly show that the number of \( d \in V \) for which \( q \mid (m^d - 1) \) is \( \frac{k}{1} + \frac{k}{2} + \frac{k}{3} + \cdots \) and that this is \( 2^k - 1 \). Use (iii) to show that \( q^r \mid Q \) for each prime divisor \( q \) of \( m^{m-1} - 1 \). Deduce that \( Q = m^{m-1} - 1 \).

(vi) Show that if \( b \) is a positive integer and \( m \geq 3 \), then \( m^b - 1 \equiv 1 \pmod{m^{b+1}} \).

(vii) Prove that the equation \( Q = m^{m-1} - 1 \) is impossible, by writing the equation in the form \( (m^{m-1} - 1) \prod_{d \in V} (m^d - 1) = \prod_{d \in T} (m^d - 1) \), and evaluating both sides \( \pmod{m^{b+1}} \) where \( b \) is the least integer of the type \( d \) that appears in the definition of \( Q \).

Proof. (i) Suppose that the sequence \((\ast m)\) has at least one prime for every positive integer \( m \) and that the sequence \((\ast m)\) does not have infinitely many primes for some integer \( m \). Let \( n \) be the least positive integer such that this happens. Let \( k \) be the largest integer such that \( 1 + kn \) is a prime. The sequence \((\ast(k + 1)n)\) is a subsequence of \((\ast m)\) and by assumption there is a prime of the form \( 1 + r(k + 1)n \), but \( r(k + 1) > k \), which is a contradiction. \( m = 1 \) gives all integers and we know there are infinitely many primes. \( m = 2 \) gives all odd integers and we know that there are infinitely many odd primes.

(ii) As \( q \) is prime, Euler’s congruence tells us that \( m^{q-1} \equiv 1 \pmod{q} \). As \( q \mid m^m - 1 \), \( m^m \equiv 1 \pmod{q} \). Now, Lemma 2.31 tells us that \( h \mid q - 1 \) and \( h \mid m \). So \( m = hc \) with \( c \geq 1 \). If \( c = 1 \), then \( h = m \) and \( h \mid q - 1 \) would imply \( m \mid q - 1 \), but we assumed there are no primes divisors \( q \) of \( m^{m-1} - 1 \) such that \( q \equiv 1 \pmod{m} \), so \( c > 1 \).

(iii) Using the formula for the sum of a geometric series, we see that

\[
m^{m-1} - 1 = m^{hc} - 1 = (m^h - 1)(1 + m^h + m^{2h} + \cdots + m^{hc})
\]

Now, \( (1 + m^h + m^{2h} + \cdots + m^{hc}) \equiv 1 + 1 + \cdots + 1 \pmod{q} \equiv c \pmod{q} \) as \( m^h \equiv 1 \pmod{q} \). As \( q \mid m^{m-1} - 1 \), \( (q, m^m) = 1 \) which implies \( (q, m) = 1 \) as \( q \) is prime. Now \( m = hc \), so we also have \( (q, c) = 1 \). This tells us that the prime factorization of the integer \( (1 + m^h + m^{2h} + \cdots + m^{hc}) \) has no power of \( q \), so if \( q^r \mid (m^h - 1) \), then \( q^r \mid (m^h - 1)(1 + m^h + m^{2h} + \cdots + m^{hc}) \). The product above tells us that \( t = r \). Now for any \( d \) such that \( h \mid d \) and \( d \mid m \), using a similar geometric series as above, we see that \( m^h - 1 \mid m^d - 1 \) and \( m^d - 1 \mid m^{m-1} - 1 \). If \( u \) is the exact power of \( q \) dividing \( m^d - 1 \), then \( m^h - 1 \mid m^d - 1 \) tells us that \( r \leq u \) and \( m^d - 1 \mid m^{m-1} - 1 \) tells us that \( u \leq r \). These two together tell us that \( u = r \).
(vi) By (ii), $q \mid m^d - 1$ if and only if $h \mid d$. $d = hc/s$. Now, $h \mid d$ if and only if $c/s$ is an integer, that is, if and only if $s \mid c$.

(v) The number of square free divisors $s$ of $c$ with $l$ distinct prime factors is $\binom{k}{l}$ (if $k > l$, we set $\binom{k}{l} = 0$) because this amounts to choosing $l$ different prime factors of $c$. By the previous part, the number of $d \in T$ for which $q \mid m^d - 1$ is the same as the number of square free divisors $s$ of $m$ which divide $c$ and have an odd number of prime factors. We can further partition this set by the number of divisors that $s$ has. So the number of square free divisors of $c$ with an odd number of prime factors is the sum of $\binom{k}{l}$ over all positive odd integers. Similarly, the number of $d \in V$ for which $q \mid m^d - 1$ is the same as the number of square free divisors $s$ of $m$ which divide $c$ and have an even number of primes factors, and this equals the sum of $\binom{k}{l}$ over all positive even integers except zero. For actually evaluating these sums, recall the binomial expansion $(1 + x)^k = \sum_{i=0}^{k} \binom{k}{i} x^i$. Plug in $x = -1$ and $x = 1$ to get $2^k = \sum_{i=0}^{k} \binom{k}{i}$ and $0 = \sum_{i=0}^{k} \binom{k}{i}(-1)^i$. Adding these equalities gives us $2(\binom{k}{0} + \binom{k}{2} + \binom{k}{4} + \cdots) = 2^k$ which simplifies to $\binom{k}{1} + \binom{k}{3} + \cdots = 2^{k-1} - 1$ and subtracting these equalities gives us that $\binom{k}{1} + \binom{k}{3} + \cdots = 2^{k-1}$.

If $s \mid c$, then $h \mid d$ and $d \mid m$, so by (iii), we have $q^r|m^d - 1$. As each $d$ in the product above is of the form $m/s$, the same geometric series argument as above tells us that $m^d - 1 \mid m^m - 1$ for every $d$, so the prime factors of $m^d - 1$ are a subset of the prime factors of $m^m - 1$. So for each prime factor $q$ of $m^m - 1$, the exact power of $q$ dividing $\prod_{d \in T}(m^d - 1)$ is $r2^{k-1}$ and the exact power of $q$ dividing $\prod_{d \in V}(m^d - 1)$ is $r(2^{k-1} - 1)$. As the only prime factors of the numerator and denominator of $Q$ are also prime factors of $m^m - 1$, we see that

$$Q = \prod_{q|m^m-1} q^{r2^{k-1}}/q^{r(2^{k-1} - 1)} = \prod_{q|m^m-1} q^r = m^m - 1$$

(vi) If $b$ is a positive integer and $m \geq 3$, then $0 < m^b - 2 < m^b < m^{b+1}$, so $m^{b+1} \nmid (m^b - 2)$ and $m^{b+1} \nmid m^b$. These can be restated as $m^b - 1 \equiv 1(\mod m^{b+1})$ and $m^b - 1 \nmid -1(\mod m^{b+1})$.

(vii) Every factor on the right hand side and left hand side apart from $m^b - 1$ is congruent to $-1$ modulo $m^{b+1}$. So multiplying these out gives $(-1)^r \equiv (-1)^t(m^b - 1)(\mod m^{b+1})$ for some positive integers $r$ and $t$. This tells us that $(m^b - 1) \equiv \pm 1(\mod m^{b+1})$ which is a contradiction.

\[Q \quad 6 \quad (3.1(4)) \quad \text{Find the values of } \left( \frac{a}{p} \right) \text{ in each of the 12 cases, } a = -1, 2, -2, 3 \text{ and } p = 11, 13, 17.\]

\[\text{Proof. By Theorem 3.1, we have to calculate } \left( \frac{a}{p} \right) = a^{(p-1)/2}(\mod p) \text{ in each case. Notice that for } a = -2, \text{ we can just multiply the results for } a = -1 \text{ and } a = 2 \text{ for a fixed prime } p. \text{ We first record the values of } a^{(p-1)/2} \text{ in a table.} \]

<table>
<thead>
<tr>
<th>$p$</th>
<th>$a$</th>
<th>$-1$</th>
<th>$2$</th>
<th>$-2$</th>
<th>$3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>-1</td>
<td>32</td>
<td>-32</td>
<td>3</td>
<td>9^49^3</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>64</td>
<td>64</td>
<td>27</td>
<td>27^2</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>16^*16</td>
<td>16^*16</td>
<td>81^*81</td>
<td></td>
</tr>
</tbody>
</table>

We can use Theorem 2.3 to simplify these. We summarize the final answer in the table below (the columns are indexed by the values of $a$ and the rows by the values of $p$, so the entry corresponding to column $a$ and row $p$ is $\left( \frac{a}{p} \right)$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$a$</th>
<th>$-1$</th>
<th>$2$</th>
<th>$-2$</th>
<th>$3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>

\[Q \quad 7 \quad (3.1(6)) \quad (a) \text{ List the quadratic residues of each of the primes } 7, 13, 17, 29, 37.\]

3
(b) For any positive integer \( n \), define \( F(n) \) to be the minimum value of \( |n^2 - 17x| \), where \( x \) runs over all integers. Prove that \( F(n) \) is either 0 or a power of 2.

Proof.  (a) If \( a \) is a primitive root modulo \( p \), then the quadratic residues are the classes of \( a^{2i} \) for \( 0 \leq i \leq (p-1)/2 \), so there are \( (p-1)/2 \) of them. As \( (p-i)^2 \equiv i^2 \pmod{p} \), the quadratic residues modulo a prime \( p \) are given by the classes of \( \{1^2, 2^2, \ldots, \left( \frac{p-1}{2} \right)^2 \} \) (these are all the quadratic residues and there are \( p-1/2 \) of them, so they are pairwise distinct). We record the answers in the tables below.

\[
p = 7
\begin{array}{c|cccc}
    x \pmod{7} & 1 & 2 & 3 \\
    x^2 \pmod{7} & 1 & 4 & 2 \\
\end{array}
\]

\[
p = 13
\begin{array}{c|cccccccc}
    x \pmod{13} & 1 & 2 & 3 & 4 & 5 & 6 \\
    x^2 \pmod{13} & 1 & 4 & 9 & 3 & 12 & 10 \\
\end{array}
\]

\[
p = 17
\begin{array}{c|cccccccccccc}
    x \pmod{17} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
    x^2 \pmod{17} & 1 & 4 & 9 & 16 & 8 & 2 & 15 & 13 \\
\end{array}
\]

\[
p = 29
\begin{array}{c|cccccccccccccccc}
    x \pmod{29} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\
    x^2 \pmod{29} & 1 & 4 & 9 & 16 & 25 & 7 & 20 & 8 & 23 & 13 & 5 & 28 & 19 & 17 \\
\end{array}
\]

\[
p = 37
\begin{array}{c|cccccccccccccccc}
    x \pmod{37} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\
    x^2 \pmod{37} & 1 & 4 & 9 & 16 & 25 & 36 & 12 & 27 & 7 & 26 & 10 & 33 & 21 & 11 & 34 & 30 & 28 & \\
\end{array}
\]

(b) Write \( n \) as \( 17q + r \) with \(-8 \leq r \leq 8\). \( |n^2 - 17x| = |r^2 - 17(x + 17q^2 + 2qr)| \). As \( x \) runs over all integers, so does \( x + 17q^2 + 2qr \). The minimum value of \( |n^2 - 17x| \) as \( x \) runs over all integers is therefore equal to the minimum value of \( |r^2 - 17y| \) as \( y \) runs over all integers. So to compute the image of the function \( F \), it suffices to calculate the images of \( \{0, 1, 2, \ldots, 8\} \). \( |a - 17x| \geq |17x| - |a| \) and \( |a - 17x| \geq |17(x - 1)| - |a - 17| \) by the triangle inequality. Therefore, for \( 0 \leq a \leq 16 \), the minimum value of \( |a - 17x| \) as \( x \) runs over all integers is \( a \) if \( 0 \leq a \leq 8 \) (\( 17|x| - a > a \) if \( x \neq 0 \)) and \( 17 - a \) if \( 9 \leq a \leq 16 \) (\( 17|x| - a > a - 17 \) if \( x \neq 1 \)). So from the table above, it is easy to see that the values of \( F(r) \) for \( 0 \leq r \leq 8 \) lie in the set \( \{0, 1, 2, 4, 8\} \).