Math 4400/6400 – Homework #8 solutions

MATH 4400 problems.

1. Let $P$ be an odd integer (not necessarily prime). Show that modulo 2,
\[
\frac{P^2 - 1}{8} \equiv \begin{cases} 
0 & \text{if } P \equiv 1, 7 \pmod{8}, \\
1 & \text{if } P \equiv 3, 5 \pmod{8}.
\end{cases}
\]

Proof. Suppose that $P \equiv 1 \pmod{8}$. Then we can write $P = 8k + 1$, and so \( \frac{P^2 - 1}{8} = \frac{(64k^2 + 16k + 1) - 1}{8} = 2(4k^2 + k) \) is even. Similarly, if $P \equiv 7 \pmod{8}$, then we can write $P = 8k - 1$, and so \( \frac{P^2 - 1}{8} = \frac{(64k^2 - 16k + 1) - 1}{8} = 2(4k^2 - k) \). If $P \equiv 3 \pmod{8}$, then we can write $P = 8k + 3$, and in this case \( \frac{P^2 - 1}{8} = 2(4k^2 + 3k) + 1 \) is odd. Finally, when $P \equiv 5 \pmod{8}$, we can write $P = 8k - 3$, and in this case \( \frac{P^2 - 1}{8} = 2(4k^2 - 3k) + 1 \) is also odd. \qed

2. Let $P, Q$ be any odd integers. Show that modulo 2,
\[
\frac{P - 1 Q - 1}{2} \equiv \begin{cases} 
0 & \text{if either } P \equiv 1 \pmod{4} \text{ or } Q \equiv 1 \pmod{4}, \\
1 & \text{if } P \equiv 3 \pmod{4} \text{ and } Q \equiv 3 \pmod{4}.
\end{cases}
\]

Proof. If $P \equiv 1 \pmod{4}$, then we can write $P = 4k + 1$, so that \( \frac{P - 1}{2} = 2k \) is even, making the product \( \frac{P - 1}{2} \frac{Q - 1}{2} \) also even. The same reasoning shows that the product is even if $Q \equiv 1 \pmod{4}$. So suppose that both $P$ and $Q$ are congruent to 3 modulo 4. Then we can write $P = 4k + 3$ and $Q = 4\ell + 3$, so that \( \frac{P - 1}{2} = 2k + 1 \) and \( \frac{Q - 1}{2} = 2\ell + 1 \) are odd. Hence, \( \frac{P - 1}{2} \frac{Q - 1}{2} \) is also odd. \qed

3. Use Gauss’s lemma to prove that for each odd prime $p$,
\[
\left( \frac{-2}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv 1, 3 \pmod{8}, \\
-1 & \text{if } p \equiv 5, 7 \pmod{8}.
\end{cases}
\]

Proof. First we prove this in the case when $p \equiv 1 \pmod{4}$. Write $p = 4k + 1$, so that \( \frac{p - 1}{2} = 2k \). Then each of the products \((-2)1, (-2)2, \ldots, (-2)k \) belongs to the interval $(-p/2, 0)$. Shifting each of them forward by $p$ (which leaves them unchanged modulo $p$), we see they are congruent to integers from the interval $(p/2, p)$. So if we write
\[
(-2)^j = \epsilon_j r_j, \quad \text{with each } \epsilon_j \in \{\pm 1\} \text{ and each } r_j \in (0, p/2),
\]
then $\epsilon_j = -1$ for all $j$ with $1 \leq j \leq k$. Now consider the remaining products \((-2)(k+1), (-2)(k+2), \ldots, (-2)(2k) \). All of these belong to the interval $(-p, -p/2)$, and so are congruent modulo $p$ to integers from the interval $(0, p/2)$. Hence, $\epsilon_j = 1$ for $k + 1 \leq j \leq 2k$. In total, there are $k$ signs which are $-1$, and so by Gauss’s lemma, \( \left( \frac{-2}{p} \right) = (-1)^k \). Thus, \( \left( \frac{-2}{p} \right) = 1 \) if $k$ is even and \( \left( \frac{-2}{p} \right) = -1 \) if $k$ is odd. The even $k$ case corresponds to $p \equiv 1 \pmod{8}$, while the odd $k$ case corresponds to $p \equiv 5 \pmod{8}$.

Now consider the case when $p \equiv 3 \pmod{4}$. Write $p = 4k + 3$, so that \( \frac{p - 1}{2} = 2k + 1 \). Then each of the products \((-2)1, (-2)2, \ldots, (-2)k \) belongs to the interval $(-p/2, 0)$,
while each of the products \((-2)(k+1), \ldots, (-2)(2k+1)\) belongs to \((-p, -p/2)\). Reasoning as before, we see that \(\epsilon_j = -1\) for \(1 \leq j \leq k\) and that \(\epsilon_j = 1\) for \(k+1 \leq j \leq 2k+1\). Again, the total number of \(-1\)s is \(k\), and so \((-2^k \over p) = (-1)^k\). Thus, \((-2^k \over p) = 1\) if \(k\) is even and \((-2^k \over p) = -1\) if \(k\) is odd. The even \(k\) case corresponds to \(p \equiv 3 \pmod{8}\), and the odd \(k\) case corresponds to \(p \equiv 7 \pmod{8}\).

4. Let \(m\) be a positive integer. By definition, there are \(\phi(m)\) integers in \([0, m)\) that are relatively prime to \(m\). Suppose we list these out, say

\[0 \leq a_1 < a_2 < a_3 < \cdots < a_{\phi(m)} < m.\]

Show that every prime \(p\) either divides \(m\) or is congruent, modulo \(m\), to one of the \(a_i\).

**Proof.** Let \(p\) be a prime number. If \(p\) does not divide \(m\), then \(p\) is relatively prime to \(m\). Let \(a\) be the remainder when \(p\) is divided by \(m\), so that \(0 \leq a < m\). Then \(p \equiv a \pmod{m}\). Moreover, you will remember from our proof of the Euclidean algorithm that \(p\) and \(a\) have the same greatest common divisor with \(m\). Thus \(\gcd(a, m) = 1\), and so \(a\) must be one of the \(a_i\).

5. Determine whether or not there is an integer \(x\) satisfying the congruence \(x^2 \equiv 116 \pmod{1009}\). **Hint:** 1009 is a prime number.

**Proof.** We have to compute \((\frac{116}{1009})\). We start off by noting that \((\frac{116}{1009}) = (\frac{116}{1009}) = (\frac{2}{1009})^2 (\frac{29}{1009}) = (\frac{29}{1009})\). Now we apply quadratic reciprocity. Since both 29 and 1009 are prime, and 29 is 1 modulo 4, we have

\[\left(\frac{29}{1009}\right) = \left(\frac{1009}{29}\right) = \left(\frac{23}{29}\right).\]

Now 23 and 29 are prime, and 29 is 1 modulo 4, so

\[\left(\frac{23}{29}\right) = \left(\frac{29}{23}\right) = \left(\frac{6}{23}\right) = \left(\frac{2}{23}\right) \left(\frac{3}{23}\right).\]

Now we know \((\frac{2}{23}) = 1\), since \(23 \equiv 7 \pmod{8}\). We also know (from an example done in class) that \((\frac{3}{23}) = 1\), since \(23 \equiv 11 \pmod{12}\). Hence, \((\frac{2}{23})(\frac{3}{23}) = 1\).

Tracing through the above reasoning shows that \((\frac{116}{1009}) = 1\), so that the congruence \(x^2 \equiv 116 \pmod{1009}\) does have a solution. (In fact, the smallest positive solution is given by \(x = 376\); this would not have been easy to find by hand!)

6. Use the law of quadratic reciprocity to determine the set of odd primes \(p\) for which \((\frac{10}{p}) = 1\). Express your answer in terms of possible residue classes of \(p\) modulo 40.

**Solution.** We ignore \(p = 5\) in what follows, since \((\frac{10}{5}) = 0\).

Notice that \((\frac{10}{p}) = (\frac{5}{p}) (\frac{2}{p})\). Thus, \((\frac{10}{p}) = 1\) if and only if \((\frac{5}{p}) = (\frac{2}{p}) = 1\) OR \((\frac{2}{p}) = (\frac{5}{p}) = -1\). As we showed in class,

\[\left(\frac{2}{p}\right) = \begin{cases} 
1 & \text{if } p \equiv 1,7 \pmod{8}, \\
-1 & \text{if } p \equiv 3,5 \pmod{8}.
\end{cases}\]
On the other hand, since \( \left( \frac{5}{p} \right) = \left( \frac{p}{5} \right) \) (by QR), and since the quadratic residues modulo 5 are 1, 4, we see that

\[
\left( \frac{5}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv 1, 4 \pmod{5}, \\
-1 & \text{if } p \equiv 2, 3 \pmod{5}.
\end{cases}
\]

(We computed this example in class.) Thus, if we want \( \left( \frac{2}{p} \right) = \left( \frac{5}{p} \right) = 1 \), we are led to solve the following four systems of congruences:

(a) \( p \equiv 1 \pmod{8} \) and \( p \equiv 1 \pmod{5} \),
(b) \( p \equiv 1 \pmod{8} \) and \( p \equiv 4 \pmod{5} \),
(c) \( p \equiv 7 \pmod{8} \) and \( p \equiv 1 \pmod{5} \),
(d) \( p \equiv 7 \pmod{8} \) and \( p \equiv 4 \pmod{5} \).

By the Chinese remainder theorem, each of these has solutions, and the solution to each is unique modulo 40. Solving the systems, we find that the solutions are

\( p \equiv 1 \pmod{40} \), \( p \equiv 9 \pmod{40} \), \( p \equiv 31 \pmod{40} \), and \( p \equiv 39 \pmod{40} \).

On the other hand, if we want \( \left( \frac{2}{p} \right) = \left( \frac{5}{p} \right) = -1 \), we are led to solve the following four systems of congruences:

(a) \( p \equiv 3 \pmod{8} \) and \( p \equiv 2 \pmod{5} \),
(b) \( p \equiv 3 \pmod{8} \) and \( p \equiv 3 \pmod{5} \),
(c) \( p \equiv 5 \pmod{8} \) and \( p \equiv 2 \pmod{5} \),
(d) \( p \equiv 5 \pmod{8} \) and \( p \equiv 3 \pmod{5} \).

Solving these systems, we get the solutions \( p \equiv 27 \pmod{40} \), \( p \equiv 3 \pmod{40} \), \( p \equiv 37 \pmod{40} \), and \( p \equiv 13 \pmod{40} \).

Putting everything together, we see that the odd primes \( p \) for which \( \left( \frac{10}{p} \right) = 1 \) are precisely those which satisfy \( p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \pmod{40} \). \( \square \)

7. (This exercise is a continuation of one on your last HW assignment.) Let \( F_n = 2^{2^n} + 1 \) be the \( n \)th Fermat number. For this exercise, we suppose that \( n \geq 2 \).

(a) Let \( p \) be a prime dividing \( F_n \). Use the exercise from your previous HW to show that \( p \equiv 1 \pmod{8} \).

\textbf{Proof.} According to the previous week’s HW, we have that \( p \equiv 1 \pmod{2^{n+1}} \). Since we are assuming that \( n \geq 2 \), we have \( n + 1 \geq 3 \), and so \( 8 \mid 2^{n+1} \mid p - 1 \). Thus, \( p \equiv 1 \pmod{8} \). \( \square \)

(b) Explain why the order of 2 modulo \( p \) divides \( \frac{p-1}{2} \).

\textbf{Proof.} Since \( p \equiv 1 \pmod{8} \), we know that 2 is a quadratic residue modulo \( p \). So by Euler’s criterion,

\[
2^{(p-1)/2} \equiv \left( \frac{2}{p} \right) \equiv 1 \pmod{p}.
\]

Thus, the order of 2 modulo \( p \) must divide \( \frac{p-1}{2} \). \( \square \)
(c) Show that $p \equiv 1 \pmod{2^{n+2}}$. This is stronger than what you concluded in your last homework, where the modulus of the congruence was $2^{n+1}$.

Proof. In last week’s HW, you determined that the order of 2 modulo $p$ was exactly $2^{n+1}$. Since the order divides $\frac{p-1}{2}$ (by part b), we see that $\frac{p-1}{2} = 2^{n+1}q$ for some $q \in \mathbb{Z}$. Hence, $p = 2^{n+2}q$, and so $p \equiv 1 \pmod{2^{n+2}}$. $\square$
MATH 6400 problems. Do two of the following three.

G1. Show that there are infinitely many primes $p$ of the form $4k + 1$.

**Proof.** Suppose for a contradiction that $p_1, p_2, \ldots, p_k$ is a complete list of primes of the form $4k + 1$. Consider the number

$$P = (2p_1 \cdots p_k)^2 + 1.$$ 

Since $P > 1$ and $p$ is odd, there is an odd prime dividing $P$. Choose one and call it $p$. Then $(2p_1 \cdots p_k)^2 \equiv -1 \pmod{p}$, so that $-1$ is a quadratic residue modulo $p$. Hence, $p$ is of the form $4k + 1$. But $p$ is not any of the $p_i$, since each $p_i \mid (2p_1 \cdots p_k)$, making $P \equiv 0^2 + 1 \equiv 1 \pmod{p_i}$, whereas $P \equiv 0 \pmod{p}$. This is a contradiction. \hfill \square

G2. If $p$ is a prime, we say that an integer $a$ not divisible by $p$ is a biquadratic residue modulo $p$ if the congruence $x^4 \equiv a \pmod{p}$ has an integer solution $x$. For a given $a$, one can ask for a characterization of the primes $p$ for which $a$ is a biquadratic residue modulo $p$. For quadratic residues, this problem is solved by the law of quadratic reciprocity; the corresponding problem for biquadratic residues is much harder! However, certain special cases can be handled in an elementary fashion. Here are two examples.

(a) Show that $-1$ is a biquadratic residue modulo the odd prime $p$ if and only if $p \equiv 1 \pmod{8}$.

**Proof.** Suppose that $x^4 \equiv -1 \pmod{p}$ for some integer $x$. Then $x^8 \equiv (-1)^2 \equiv 1 \pmod{p}$. From these two congruences, we can read off that the order of $x$ modulo $p$ divides 8 but does not divide 4. It follows that $x$ has order 8 modulo $p$. Since the order divides $p-1$, we get that $p \equiv 1 \pmod{8}$.

On the other hand, suppose that $p \equiv 1 \pmod{8}$. Let $a$ be a primitive root mod $p$, and let $x = a^{(p-1)/8}$. Then $a$ has order $p-1$, $x$ has order 8, and $x^4$ has order 2. But the only element of order 2 modulo an odd prime $p$ is $-1$. Thus, $x^4 \equiv -1 \pmod{p}$, making $-1$ is a biquadratic residue. \hfill \square

(b) Show that $-4$ is a biquadratic residue modulo the odd prime $p$ if and only if $p \equiv 1 \pmod{4}$.

**Proof.** Suppose that $p \equiv 1 \pmod{4}$. Choose an $x \in \mathbb{Z}$ with $x^2 \equiv -1 \pmod{p}$. Then $(1 + x)^2 \equiv 1 + 2x + x^2 \equiv 2x \pmod{p}$, and $(1 + x)^4 \equiv (2x)^2 = 4x^2 \equiv -4 \pmod{p}$. So $-4$ is a biquadratic residue mod $p$.

Conversely, suppose that $-4$ is a biquadratic residue modulo $p$. Choose $x \in \mathbb{Z}$ with $x^4 \equiv -4 \pmod{p}$. Then $p \mid x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$, and so either $p \mid x^2 + 2x + 2$ or $p \mid x^2 - 2x + 2$. In the first case, $(x + 1)^2 \equiv -1 \pmod{p}$, and in the second case, $(x - 1)^2 \equiv -1 \pmod{p}$. Either way, $-1$ is a quadratic residue modulo $p$, and so $p \equiv 1 \pmod{4}$. \hfill \square

G3. Let $F_n = 2^{2^n} + 1$. Show that the following criterion holds for all $n \geq 1$:

$$F_n \text{ is prime} \iff 3^{F_n-1} \equiv -1 \pmod{F_n}.$$
Proof. Suppose that $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$. Let $K = \frac{F_n-1}{2}$. Then $3^K \equiv -1 \pmod{F_n}$, so that $3^{2K} \equiv 1 \pmod{F_n}$. Hence, the order of $3$ modulo $F_n$ divides $2K$ but not $K$. However, $K = 2^{n-1}$ is a power of 2, and so the only positive integer dividing $2K$ but not $K$ is $2K$. So $3$ has order $2K = F_n - 1$ modulo $F_n$. Thus, $F_n - 1$ divides the size of the unit group mod $F_n$. But the size of the unit group mod $F_n$ is smaller than $F_n$ unless $F_n$ is prime. This proves the $\Leftarrow$ direction.

For the $\Rightarrow$ direction, we first determine $F_n$ modulo 12. Notice that $F_1 = 5 \equiv 5 \pmod{12}$. But whenever $F_n \equiv 5 \pmod{12}$, we have $F_{n+1} = (F_n - 1)^2 + 1 \equiv 4^2 + 1 \equiv 17 \equiv 5 \pmod{12}$. So by induction, each $F_n \equiv 5 \pmod{12}$. So if $F_n$ is prime, then \( \left( \frac{3}{F_n} \right) = -1 \). By Euler’s criterion,

\[
3^{\frac{F_n-1}{2}} \equiv \left( \frac{3}{F_n} \right) \equiv -1 \pmod{F_n}.
\] 

\[\Box\]