Math 580, Exam 2. 10/21/09. Name: ______________________

• Read problems carefully. Show all work.
• No notes, calculator, or text.
• The exam is approximately 15 percent of the total grade.
• There are 100 points total. Partial credit may be given.
1. *(25 points)*

(a) *(10 points)* Find all incongruent solutions mod 44 to the linear congruence

\[ 19x \equiv 8 \pmod{44}. \]

**Solution:** \( \gcd(19, 44) = 1 \mid 8 \implies \) there is one solution mod 44.

\[ 19x \equiv 8 \pmod{44} \implies \exists k \in \mathbb{Z} \text{ with } 19x - 44k = 8. \] We solve \( 19x - 44k = 1 \) as follows.

\[ 44 = 2 \cdot 19 + 6 \]
\[ 19 = 3 \cdot 6 + 1 \]

We have:

\[ 1 = 19 - 3 \cdot 6 = 19 - 3 \cdot (44 - 2 \cdot 19) = 19 \cdot 7 - 44 \cdot 3 \]

Multiplying by 8 gives

\[ 19 \cdot 56 - 44 \cdot 21 = 7, \]

from which it follows that \( x \equiv 56 \equiv 12 \pmod{44}. \)

(b) *(8 points)* How many incongruent solutions mod 51 does the linear congruence

\[ 17x \equiv 34 \pmod{51} \]

have? Briefly explain. I am not asking you to find the solutions (if any exist).

**Solution:** \( \gcd(17, 51) = 17 \mid 34 \implies \) there are 17 solutions modulo 51.

(c) *(7 points)* How many incongruent solutions mod 68 does the linear congruence

\[ 52x \equiv 14 \pmod{68} \]

have? Briefly explain. I am not asking you to find the solutions (if any exist).

**Solution:** We have

\[ 68 = 1 \cdot 52 + 16 \]
\[ 52 = 3 \cdot 16 + 4 \]
\[ 16 = 4 \cdot 4 \implies \gcd(52, 68) = 4. \]

Since \( 4 \nmid 14 \), there are no solutions.
2. (20 points) Solve the following system of linear congruences.

\[ x \equiv 3 \pmod{4} \]
\[ x \equiv 2 \pmod{7} \]
\[ x \equiv 7 \pmod{9}. \]

You may leave your answer as a \textbf{sum of products (unsimplified)}. 

\textbf{Solution:}

- \[ 7 \cdot 9 \cdot x_1 \equiv 1 \pmod{4} \iff 63x_1 \equiv 3x_1 \equiv 1 \pmod{4} \iff x_1 \equiv 3 \pmod{4}. \]
- \[ 4 \cdot 9 \cdot x_2 \equiv 1 \pmod{7} \iff 36x_2 \equiv x_2 \equiv 1 \pmod{7}. \]
- \[ 4 \cdot 7 \cdot x_3 \equiv 1 \pmod{9} \iff 28x_3 \equiv x_3 \equiv 1 \pmod{9}. \]

Now, the solution is

\[ x \equiv (7 \cdot 9 \cdot 3) + (4 \cdot 9 \cdot 1) \cdot 2 + (4 \cdot 7 \cdot 1) \cdot 7 \equiv 567 + 72 + 196 \equiv 835 \equiv 79 \pmod{252 = 4 \cdot 7 \cdot 9}. \]

\textbf{Note:} You can check your answer.

\[ 79 \equiv 3 \pmod{4} \]
\[ 79 \equiv 2 \pmod{7} \]
\[ 79 \equiv 7 \pmod{9}. \]
3. (20 points)

(a) (10 points) Let \( n \) be a positive integer. Show that \( 17 \mid 3 \cdot 5^{2n+1} + 2^{3n+1} \).

Solution: We have

\[
3 \cdot 5^{2n+1} + 2^{3n+1} = 3 \cdot 25^n \cdot 5 + 8^n \cdot 2 \\
\equiv 15 \cdot 8^n + 2 \cdot 8^n \\
\equiv 17 \cdot 8^n \equiv 0 \pmod{17}.
\]

(b) (10 points) Use Fermat’s Little Theorem to compute \( 3^{226} \pmod{23} \).

Solution: Since \( \gcd(3, 23) = 1 \), Fermat’s Little Theorem \( \implies \)

\[
3^{22} \equiv 1 \pmod{23}.
\]

We also note that \( 226 = 10 \cdot 22 + 6 \). It follows that

\[
3^{226} = (3^{22})^{10} \cdot 3^6 \equiv 3^6 \pmod{23}.
\]

But also, we have

\[
3^3 = 27 \equiv 4 \pmod{23} \implies 3^6 = (3^3)^2 \equiv 4^2 \equiv 16 \pmod{23}.
\]

Hence, we have \( 3^{226} \equiv 16 \pmod{23} \).
4. (20 points)

(a) (5 points) One of the following statements is true. Circle the true statement. Cite a theorem from class to justify your answer.

- There are infinitely many primes of the form $15n + 6$.
- There are infinitely many primes of the form $20n + 9$.

**Solution:** $\gcd(15, 6) = 3; \gcd(20, 9) = 1$. Hence, Dirichlet’s Theorem $\implies$ there are infinitely many primes of the form $20n + 9$.

(b) (5 points) State Bertrand’s Postulate. It is sometimes called Bertrand’s Conjecture (but it is actually a theorem).

**Solution:** For all $n \geq 2$, there is a prime $p$ with $n < p < 2n$.

(c) (10 points) Let $n > 1$ be an integer. Use Bertrand’s Postulate to show that $n!$ is not a perfect square. (In other words, $n! \neq m^2$ for any integer $m$.)

**Solution:** Note that $n!$ is square $\iff$ the power of all primes $p$ dividing $n!$ is even.

- $n$ even $\implies$ $\exists$ prime $p$ with $n/2 < p < n$. The power of this prime in the factorization of $n!$ is one (odd). Hence, $n!$ is not square.
- $n$ odd $\implies$ $\exists$ prime $p$ with $(n + 1)/2 < p < n + 1$ The power of this prime in the factorization of $n!$ is one (odd). Hence, $n!$ is not square.
5. **(15 points)** Suppose that $p$ and $q$ are distinct odd primes, that $a \in \mathbb{Z}$, and that $\gcd(a, pq) = 1$. Prove that

$$a^{(p-1)(q-1)+1} \equiv a \pmod{pq}.$$  

**Solution:** $\gcd(a, pq) = 1 \implies p \nmid a$, so by Fermat’s Little Theorem, we have

$$a^{p-1} \equiv 1 \pmod{p} \implies a^{(p-1)(q-1)+1} \equiv (a^{p-1})^{q-1} \cdot a \equiv 1 \cdot a \equiv a \pmod{p}.$$  

Similarly, $\gcd(a, pq) = 1 \implies q \nmid a$; by the same reasoning, we find that $a^{(p-1)(q-1)+1} \equiv a \pmod{q}$. Now, since $p$ and $q$ are distinct primes, the result follows (by, for example, the Chinese Remainder Theorem).