**Calculator policy.** You may use a calculator to perform arithmetic computations, but you may not use a calculator or other device to execute number theoretic algorithms (such as computing gcds, applying the Chinese Remainder Theorem, solving linear Diophantine equations, etc).

## Skills Questions [60 points]

**Directions:** Solve 4 of the following 6 problems.

1. Total Recall. Complete two of the following three tasks.
   (a) Carefully give the definition of a prime number.
   (b) State the Fundamental Theorem of Arithmetic (FTA).
   (c) State the Chinese Remainder Theorem (CRT).
2. Express the number $73,614$ in base 8.
3. Recall that the (multiplicative) inverse of $a$ modulo $m$ is an integer $\tilde{a}$ such that $a\tilde{a} \equiv 1 \pmod{m}$. Let $m = 11607$ and let $a = 5288$. Use the Extended Euclidean Algorithm to find the inverse of $a$ modulo $m$.
4. The following system does not satisfy the hypotheses of the Chinese Remainder Theorem. Convert the system to an equivalent one that does satisfy the hypotheses of the CRT. *Do not solve the system.*

$$2x \equiv 8 \pmod{15} \qquad 5x \equiv 17 \pmod{21} \qquad 6x \equiv 18 \pmod{22}$$

5. Find the set of all solutions to $735x + 1729y = 28$.
6. Is there a reduced residue system $R$ modulo 9 such that each element in $R$ is an odd prime? Either find such a system or show that one does not exist.

## Deeper Questions [40 points]

**Directions:** Solve 2 of the following 3 problems.

1. It is well known that an integer $n$ is divisible by 3 if and only if the base-10 digits of $n$ sum to a multiple of 3. Find and prove an analogous rule that characterizes when $n$ is divisible by 3 in terms of the base-8 digits of $n$.
2. Show that if $\gcd(a, m) = 1$ and $\gcd(a-1, m) = 1$, then $1+a+a^2+\cdots+a^{\phi(m)-1} \equiv 0 \pmod{m}$.
3. An integer $a$ is a *self-inverse* modulo $m$ if $a^2 \equiv 1 \pmod{m}$.
   (a) Let $p$ be an odd prime and let $e$ be a positive integer. Prove that $a^2 \equiv 1 \pmod{p^e}$ if and only if $a \equiv -1 \pmod{p^e}$ or $a \equiv 1 \pmod{p^e}$.
   (b) Let $m$ be an odd integer with $m \geq 3$. Prove that the number of self-inverses modulo $m$ equals $2^t$, where $t$ is the number of primes dividing $m$.