Notes for Recitation 4

Problem 1. A number is perfect if it is equal to the sum of its positive divisors, other than itself. For example, 6 is perfect, because $6 = 1 + 2 + 3$. Similarly, 28 is perfect, because $28 = 1 + 2 + 4 + 7 + 14$. Prove that $2^{k-1}(2^k - 1)$ is perfect when $2^k - 1$ is prime.

All even perfect numbers are known to have this form. Whether or not there exists an odd perfect number has been an open question for more than two thousand years.

Solution. If $2^k - 1$ is prime, then the only divisors of $2^{k-1}(2^k - 1)$ are:

$$1, 2, 4, \ldots, 2^{k-1}$$

which sum to $2^k - 1$ and

$$1 \cdot (2^k - 1), 2 \cdot (2^k - 1), 4 \cdot (2^k - 1), \ldots, 2^{k-2} \cdot (2^k - 1)$$

which sum to $(2^{k-1} - 1) \cdot (2^k - 1)$. Adding these two sums gives $2^{k-1}(2^k - 1)$, so the number is perfect.

Problem 2. Many divisibility tests are rooted in modular arithmetic.

(a) Use induction to prove that $10^k \equiv 1 \pmod{9}$ for all $k \geq 0$.

Solution. We use induction. Let $P(k)$ be the proposition that $10^k \equiv 1 \pmod{9}$.

Base case: $P(0)$ is true because $10^0 = 1$, which is congruent to 1.

Inductive step: Assume that $P(k)$ is true, where $k \geq 0$. Then $P(k + 1)$ is also true by the following reasoning:

$$10^{k+1} \equiv 10 \cdot 10^k \pmod{9}$$

$$\equiv 10 \cdot 1 \pmod{9}$$

$$\equiv 1 \pmod{9}$$

The first step uses the induction hypothesis and the second is simplification. The claim follows by the induction principle.

(b) Prove that a number written in decimal is divisible by 9 if and only if the sum of its digits is a multiple of 9.

Solution. A number in decimal has the form:

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0$$
From the observation above, we know:
\[ d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 \equiv d_k + d_{k-1} + \ldots + d_1 + d_0 \pmod{9} \]

This shows that the remainder when the original number is divided by 9 is equal to the remainder when the sum of the digits is divided by 9. In particular, if one is zero, then so is the other.

**Problem 3.** Suppose that \( p \) is a prime.

(a) An integer \( k \) is **self-inverse** if \( k \cdot k \equiv 1 \pmod{p} \). Find all integers that are self-inverse mod \( p \).

**Solution.** The congruence holds if and only if \( p \mid k^2 - 1 \) which is equivalent to \( p \mid (k + 1)(k - 1) \). This holds if and only if either \( p \mid k + 1 \) or \( p \mid k - 1 \). Thus, \( k \equiv \pm 1 \pmod{p} \).

(b) **Wilson’s Theorem** says that \( (p-1)! \equiv -1 \pmod{p} \). The English mathematician Edward Waring said that this statement would probably be extremely difficult to prove because no one had even devised an adequate notation for dealing with primes. (Gauss proved it while standing.) Your turn! Stand up, if you like, and try cancelling terms of \( (p-1)! \) in pairs.

**Solution.** If \( p = 2 \), then the theorem holds, because \( 1! \equiv -1 \pmod{2} \). If \( p > 2 \), then \( p - 1 \) and 1 are distinct terms in the product \( 1 \cdot 2 \cdots (p-1) \), and these are the only self-inverses. Consequently, we can pair each of the remaining terms with its multiplicative inverse. Since the product of a number and its inverse is congruent to 1, all of these remaining terms cancel. Therefore, we have:

\[
(p-1)! \equiv 1 \cdot (p-1) \pmod{p} \\
\equiv -1 \pmod{p}
\]

**Problem 4.** We’ve noted that many assertions about the real numbers have analogues in the integers modulo a prime. Here is another example. Two nonparallel lines in the real plane intersect at a point. Algebraically, this means that the equations

\[
y = m_1 x + b_1 \\
y = m_2 x + b_2
\]

have a unique solution \( (x, y) \), provided \( m_1 \neq m_2 \). This statement would be false if we restricted \( x \) and \( y \) to the integers, since the two lines could cross at a noninteger point:
However, an analogous statement holds if we work over the integers \textit{modulo a prime} \( p \). Find a solution to the congruences

\[
\begin{align*}
y & \equiv m_1 x + b_1 \pmod{p} \\
y & \equiv m_2 x + b_2 \pmod{p}
\end{align*}
\]

of the form \( x \equiv ? \pmod{p} \) and \( y \equiv ? \pmod{p} \) where the ?’s denote expressions involving \( m_1, m_2, b_1, \) and \( b_2 \). You may find it helpful to solve the original equations over the reals first.

\textbf{Solution.} Subtracting the second congruence from the first, we have:

\[
\begin{align*}
0 & \equiv m_1 x + b_1 - (m_2 x + b_2) \pmod{p} \\
(m_1 - m_2) x & \equiv b_2 - b_1 \pmod{p} \\
x & \equiv (m_1 - m_2)^{-1} \cdot (b_2 - b_1) \pmod{p}
\end{align*}
\]

Substituting this value of \( x \) into the first congruence, we have

\[
y \equiv m_1 \cdot (m_1 - m_2)^{-1} \cdot (b_2 - b_1) + b_1 \pmod{p}
\]