1. Practice problems

**Problem 1.** Solve $97x \equiv 13 \pmod{105}$.

*Proof.* We first use Euclidean algorithm to find a multiplicative inverse of 97 modulo 105:

\[
\begin{align*}
105 &= 1 \times 97 + 8 \\
97 &= 12 \times 8 + 1 \\
8 &= 8 \times 1 + 0
\end{align*}
\]

Therefore, $1 = 97 - 12 \times 8 = 97 - 12 \times (105 - 97) = 13 \times 97 - 12 \times 105$. It follows that $13 \times 97 \equiv 1 \pmod{105}$. We can now solve

\[
\begin{align*}
97x &\equiv 13 \pmod{105} \\
13 \times 97x &\equiv 13^2 \pmod{105} \\
x &\equiv 169 \pmod{105} \\
x &\equiv 64 \pmod{105}
\end{align*}
\]

\[\square\]

**Remark.** The Euclidean algorithm computation above gives $\frac{105}{97} = (1, 12, 8)$.

**Problem 2.** Let $p \geq 5$ be an odd prime and consider numbers $a_1 = 1, a_2 = 2, \ldots, a_{p-1} = p - 1$. Prove that $p$ divides

\[\sum_{i<j} a_ia_j.\]

*Solution 1:* The key observation is that

\[\begin{align*}
(a_1 + a_2 + \cdots + a_{p-1})^2 &= a_1^2 + a_2^2 + \cdots + a_{p-1}^2 + 2\sum_{i<j} a_ia_j.
\end{align*}\]

Recall that

\[1 + 2 + \cdots + (p-1) = p(p-1)/2\]

and

\[1^2 + 2^2 + \cdots + (p-1)^2 = p(p-1)(2p-1)/6.\]

Therefore, we can compute

\[2\sum_{i<j} a_ia_j = (p(p-1)/2)^2 - p(p-1)(2p-1)/6.\]

Since $p \geq 5$ is an odd prime, it follows that $p$ divides $\sum_{i<j} a_ia_j$. \[\square\]

**Problem 3.** Let $p \geq 5$ be a prime. Prove that $(p-3)! \equiv (p-1)/2 \pmod{p}$. 

Proof. By Wilson’s theorem
\[(p - 1)! \equiv -1 \pmod{p}\]
or
\[(p - 1)(p - 2)(p - 3)! \equiv -1 \pmod{p}.
\]This gives \(-2(p - 3)! \equiv 1 \pmod{p}\). Since \(-2(p - 1)/2 \equiv 1 \pmod{p}\), we conclude that \((p - 3)! \equiv (p - 1)/2 \pmod{p}\).

\[\square\]

Problem 4. Solve the congruence \(x^2 \equiv 17 \pmod{64}\).

Proof. This problem is in the spirit of the Hensel’s lemma. We begin with an observation that \(x^2 \equiv 17 \pmod{16}\) has many solutions. Namely, \(x^2 \equiv 17 \equiv 1 \pmod{16}\) exactly when \(x \equiv \pm 1 \pmod{8}\). We will now attempt to construct solutions of \(x^2 \equiv 17 \pmod{64}\). Suppose \(x = 8k + 1\). Then
\[x^2 - 17 = 64k^2 + 16k - 16 \equiv 16(k - 1) \pmod{64}.
\]This means that \(x^2 - 17\) is divisible by 64 if and only if \(k \equiv 1 \pmod{4}\). We conclude that \(x = 8k + 1 = 8(4\ell + 1) + 1 = 32\ell + 9\) for some integer \(\ell\).

Suppose \(x = 8k - 1\). Then
\[x^2 - 17 = 64k^2 - 16k - 16 \equiv -16(k + 1) \pmod{64}.
\]This means that \(x^2 - 17\) is divisible by 64 if and only if \(k \equiv -1 \pmod{4}\). We conclude that \(x = 8k - 1 = 8(4\ell - 1) - 1 = 32\ell - 9\) for some integer \(\ell\).

Summarizing \(x \equiv \pm 9 \pmod{32}\) is the solution of the congruence \(x^2 \equiv 17 \pmod{64}\).

\[\square\]

Problem 5. Find all integers \(x\) satisfying \(x \equiv 2 \pmod{3}, x \equiv 3 \pmod{4}, x \equiv 4 \pmod{5}, x \equiv 5 \pmod{6}\).

Proof. The Chinese Remainder Theorem says that the system
\[
\begin{align*}
x &\equiv 2 \pmod{3} \\
x &\equiv 3 \pmod{4} \\
x &\equiv 4 \pmod{5}
\end{align*}
\]has a unique solution modulo 60, namely \(x \equiv 59 \pmod{60}\). Clearly, this solution also satisfies \(x \equiv 5 \pmod{6}\). We are done.

\[\square\]

Problem 6. Suppose \(n\) is such that \(2^n - 1\) is a prime. Prove that \(n\) is also a prime.

Historical reference: Prime numbers of the form \(M_p = 2^p - 1\) where \(p\) is a prime are called Mersenne primes. Presently, only 48 Mersenne primes are known. The largest, found in February 2013, is
\[M_{57,885,161} = 2^{57,885,161} - 1.\]
Solution: Suppose not. Then \( n = ab \) for some positive integers \( a, b \geq 2 \). We compute
\[
2^n - 1 = (2^a)^b - 1 = (2^a - 1) \left( (2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1 \right).
\]
A contradiction! \( \square \)

**Problem 7.** We say that a number \( n \) is **perfect** if it is the sum of all its divisors, including 1 but excluding \( n \) itself:
\[
n = \sum_{1 \leq d \leq n, d | n} d.
\]
For example, 6 is perfect because 6 = 1 + 2 + 3.

Prove that for odd primes \( p \) and \( q \), \( p^aq^b \) cannot be perfect.

**Historical reference:** Euclid observed that if \( p = 2^{a-1} - 1 \) is a Mersenne prime, then \( 2^{a-1}n \) is perfect. Euler proved that every even perfect number is of this form. It is not known if there are any odd perfect numbers.

**Proof.** Consider first the case when \( p = q \). Then \( n = p^c \) and the divisors of \( n \) less than \( n \) are 1, \( p \), \ldots, \( p^{c-1} \). We have
\[
1 + p + \cdots + p^{c-1} = \frac{p^c - 1}{p - 1} \neq p^c
\]
because \( (p - 2)p^c \neq -1 \).

Suppose now \( p \neq q \). We use a simple observation that \( n \) is perfect if and only if the sum of all positive divisors of \( n \) is 2\( n \).

The divisors of \( n = p^aq^b \) are precisely \( p^aq^j \), where \( i \leq a, j \leq b \). It is easy to see that the sum of all divisors of \( n \) is then
\[
(1 + p + p^2 + \cdots + p^a)(1 + q + q^2 + \cdots + q^b) = \left( \frac{p^{a+1} - 1}{p - 1} \right) \left( \frac{q^{b+1} - 1}{q - 1} \right).
\]
Suppose \( n \) is perfect, then
\[
\left( \frac{p^{a+1} - 1}{p - 1} \right) \left( \frac{q^{b+1} - 1}{q - 1} \right) = 2p^aq^b
\]
Simplifying:
\[
p^{a+1}q^{b+1} - q^{b+1} - p^{a+1} + 1 = 2p^{a+1}q^{b+1} - 2p^{a+1}q^b - 2p^aq^{b+1} + 2p^aq^b,
\]
or
\[
p^{a+1}q^{b+1} - 2p^{a+1}q^b - 2p^aq^{b+1} + q^{b+1} + p^{a+1} + 2p^aq^b - 1 = 0
\]
\[
(p^{a+1} - 2p^a)(q^{b+1} - 2q^b) + q^{b+1} + q^{b+1} - 2p^aq^b = 1
\]
\[
p^aq^b(p - 2)(q - 2) + q^{b+1} + q^{b+1} - 2p^aq^b = 1
\]
This is clearly absurd. \( \square \)
Problem 8. Suppose \( p \) is a prime number such that \( (p - 1)/4 \) is also a prime. Prove that 2 is a primitive root modulo \( p \).

**Proof.** We first directly verify that 2 is a primitive root modulo 3 and 5. From now on, assume that \( p \) is greater than 5. (Of course, this is already implicit in the assumption that \( (p - 1)/4 \) is a prime.)

Note that \( p - 1 = 2^2 \left( \frac{p+1}{4} \right) \) is a prime factorization of \( p - 1 \). It follows that the order of 2 modulo \( p \) is one of the following numbers: \( p - 1, (p - 1)/2, (p - 1)/4, 2, 4 \). If the order divides 4, then \( p \mid 2^4 - 1 = 15 \), which is impossible by our assumption \( p > 5 \).

Suppose the order divides \( (p - 1)/2 \). Then \( 2^{(p-1)/2} \equiv 1 \pmod{p} \). By Euler’s criterion, this implies that 2 is a quadratic residue modulo \( p \). The quadratic reciprocity law then says that \( p \equiv \pm 1 \pmod{8} \). If \( p \equiv -1 \pmod{8} \), then \( (p - 1)/4 \) is not even an integer. If \( p \equiv 1 \pmod{8} \), then \( (p - 1)/4 \) is even, so cannot be a prime (\( p \neq 9! \)). We have arrived at a contradiction!

It follows that the only possibility for the order of 2 is \( p - 1 \), which means that 2 is a primitive root of \( p \). \( \square \)

Problem 9. Suppose \( g \) is a primitive root modulo \( p^2 \). Prove that \( g \) is also a primitive root modulo \( p \).

**Proof.** Suppose not. Then the order of \( g \) modulo \( p \) is \( d \), where \( d \mid p - 1 \) and \( d < p - 1 \). We have \( g^d \equiv 1 \pmod{p} \) and so \( g^d = 1 + pk \) for some integer \( k \). Raise this equality to the power \( p \):

\[
g^{dp} = (1 + pk)^p = 1 + p^2 k + \left( \frac{p}{2} \right)(pk)^2 + \cdots + (pk)^p \equiv 1 \pmod{p^2}.
\]

It follows that the order of \( g \) modulo \( p^2 \) divides \( dp \). However, the order of \( g \) modulo \( p^2 \) is \( p(p - 1) \) by assumption. We have arrived at a contradiction and so \( g \) is a primitive root of \( p \). \( \square \)

Problem 10. Find the continued fraction expansion of \( \sqrt{n^2 + 1} \).

**Proof.** Let \( x = n + \sqrt{n^2 + 1} \). Then

\[
x = 2n + (\sqrt{n^2 + 1} - n) = 2n + \frac{1}{\sqrt{n^2 + 1} + n} = 2n + \frac{1}{x}.
\]

It follows that \( x = \langle 2n \rangle \) and so \( \sqrt{n^2 + 1} = \langle n, 2n \rangle \). \( \square \)