Midterm 1 will cover the material of all lectures up to and including February
14. More precisely, the following topics are covered:

1. Divisibility. Division algorithm.
2. Euclidean algorithm. Greatest common divisors.
3. Prime numbers.
4. Uniqueness of factorization.
7. Euler’s $\phi$-function.
10. Euler’s criterion.

To prepare for the midterm, review your lecture notes and redo the first three
problems sets (also read and work through the posted solutions).

Here are a few extra practice problems:

**Problem 1.** Find the greatest common divisor of 72 and 231. Write it in the form
d = 72x + 231y.

*Solution:* Applying Euclidean algorithm, we obtain:

\[
231 = 3 \times 72 + 15, \\
72 = 4 \times 15 + 12, \\
15 = 1 \times 12 + 3, \\
12 = 4 \times 3 + 0.
\]

It follows that \((231, 72) = 3\). We have

\[
3 = 15 - 12 = 15 - (72 - 4 \times 5) = 5 \times 15 - 72 = 5 \times (231 - 3 \times 72) - 72 = 5 \times 231 - 16 \times 72
\]

**Problem 2.** Write 1 as a linear combination of 12 and 5. What is the multiplicative
inverse of 5 modulo 12?

*Solution:* Since \((12, 5) = 1\), Euclidean algorithm gives 1 = 5 \times 5 - 2 \times 12. In
particular, \(1 \equiv 5 \times t \pmod{12}\). It follows that the multiplicative inverse of 5
modulo 12 is 5.

**Problem 3.** Find a number \(x\) which satisfies

\[
\begin{cases}
  x \equiv 5 \pmod{7} \\
  x \equiv 2 \pmod{4} \\
  x \equiv 2 \pmod{3}
\end{cases}
\]

*Solution:* First one finds that

1. \(b_1 = 3\) is the multiplicative inverse of 12 modulo 7.
2. \(b_2 = 1\) is the multiplicative inverse of 21 modulo 4.
3. \(b_3 = 1\) is the multiplicative inverse of 28 modulo 3.
Then the algorithmic version of Chinese Remainder Theorem gives the solution as
\[ x = 5 \times b_1 \times 12 + 2 \times b_2 \times 21 + 2 \times b_3 \times 28 = 180 + 42 + 56 \equiv 26 \pmod{84} \]

Problem 4. Let \( p \) be a prime. For which values of \( k \) does \( p \) divide \( \binom{p}{k} \)?

Solution:
\[ \binom{p}{0} = \binom{p}{p} = 1 \]

Hence \( k = 0 \) and \( k = p \) are ruled out. We will show that for all \( 1 \leq k \leq p - 1 \), \( \binom{p}{k} \) is divisible by \( p \). To do this, recall that
\[ \binom{p}{k} = \frac{p!}{k!(p-k)!} \]

Now, \( p! = p(p-1)\cdots 1 \) is divisible by \( p \). Since \( p \) is a prime and \( k \leq p - 1 \) and \( p - k \leq p - 1 \), we have that \( k! = k(k-1)\cdots 1 \) and \( (p-k)! = (p-k)(p-k-1)\cdots 1 \) are not divisible by \( p \). It follows that the integer \( \frac{p!}{k!(p-k)!} \) must be divisible by \( p \). □

Problem 5. Which of the following numbers are representable as a sum of two integer squares: 41, 122, 150?

Solution: A prime number \( p \) is representable as a sum of squares if and only if \( p \equiv 1 \pmod{4} \). A composite number \( n \) is representable as a sum of squares if and only if all prime divisors of \( n \) that are congruent to 3 \pmod{4} \) appear with an even exponent in the prime factorization of \( n \).

Since 41 is prime and 41 \( \equiv 1 \pmod{4} \), 41 is a sum of two squares. In fact, 41 = 5^2 + 4^2.

Since 122 = 2 × 61 and 61 is a prime congruent to 1 modulo 4, 122 is a sum of two squares. In fact, 122 = 11^2 + 1^2.

Since 150 = 2 × 3 × 5^2 and 3 \equiv 3 \pmod{4} \), we conclude that 150 is not a sum of two squares. □

Problem 6. Give a definition of Euler’s \( \phi \)-function. Compute \( \phi(360) \).

Solution: \( \phi(n) \) is a number of integers between 0 and \( n \) that are coprime to \( n \). If \( n = p_1^{r_1} \cdots p_k^{r_k} \) is a prime factorization of \( n \), then
\[ \phi(n) = (p_1 - 1) \cdots (p_k - 1)p_1^{r_1 - 1} \cdots p_k^{r_k - 1} . \]

Since 360 = 2^3 × 3^2 × 5, we see that
\[ \phi(360) = (2 - 1)(3 - 1)(5 - 1)2^23^15^0 = 96. \]

Problem 7. Does equation \( x^4 - x^3 + 1 = 0 \) have any integer solutions?

Solution: No, the number \( x^4 - x^3 \) is always even. Hence \( x^4 - x^3 + 1 \) is always odd. □

Problem 8. Solve \( x^3 - 2x + 4 \equiv 0 \pmod{3^3} \).
Solution: The only solution of $x^3 - 2x + 4 \equiv 0 \pmod{3}$ is $x \equiv 1 \pmod{3}$. Since $f'(x) = (x^3 - 2x + 4)' = 3x^2 - 2 \equiv 1 \not\equiv 1 \pmod{3}$, Hensel’s lemma says that the unique solution modulo 3 lifts uniquely to a solution modulo $3^3$.

The multiplicative inverse of $f'(1)$ modulo 3 is 1. Hence $x \equiv 1 \pmod{3}$ lifts to $x \equiv 1 - f(1) = -2 \pmod{9}$ or $x \equiv 7 \pmod{9}$. In turns, this lifts to $x \equiv 7 - f(7) = 7 - 333 \equiv 2 \pmod{2}$ or $x \equiv 25 \pmod{2}$.

Remark. Another way to go about this particular example is to observe that $x^3 - 2x + 4 = 0$ has an integer root $x = -2$.

Problem 9. Let $p > 2$ be a prime. Prove that the map $x \mapsto x^{p-2}$ is a bijection of the complete residue system modulo $p$ onto itself.

Proof. Since we consider a map from a set to itself, to prove that the map is a bijection it suffices to show that the map is an injection.

Clearly, 0 maps to 0 and $x^{p-2} \equiv 0$ if and only if $x \equiv 0$. It remains to show that the map $x \mapsto x^{p-2}$ is injective when restricted to the set of non-zero residues. Suppose $x_1^{p-2} \equiv x_2^{p-2} \pmod{p}$ for some $x_1, x_2 \not\equiv 0 \pmod{p}$. Then by Fermat’s little theorem,

$$x_2 \equiv x_1^{p-1} x_2 \equiv x_1 x_1^{p-2} x_2 \equiv x_1 x_2^{p-2} x_2 \equiv x_1 x_2 x_2 x_2^{p-1} \equiv x_1 \pmod{p}.$$ 

This finishes the proof of injectivity.