1. Material covered

(1) Divisibility. Division algorithm.
(2) Euclidean algorithm. Greatest common divisors.
(3) Prime numbers.
(4) Uniqueness of factorization.
(6) Fermat’s little theorem. Wilson’s theorem.
(7) Euler’s $\phi$-function.
(8) Chinese Remainder Theorem.
(9) Algebraic congruences. Hensel’s lemma.
(10) Primitive roots of prime numbers.
(11) Solving algebraic congruences $x^a \equiv b \pmod{p}$.
(12) Quadratic residues.
(13) Euler’s criterion.
(14) Legendre’s symbol.
(15) Gauss’ lemma.
(16) Quadratic reciprocity laws.
(17) Continued fractions.
(18) Representation of rational numbers by simple continued fraction using Euclidean algorithm.
(19) Infinite continued fractions.
(20) Representation of quadratic irrationals by periodic infinite continued fractions.
(21) Solving Pell’s equation using continued fractions.
(22) RSA algorithm.
(23) Primality testing. Probable primes.
(24) Existence of primitive roots modulo $p^\alpha$, $p$ an odd prime.
(25) Carmichael numbers.
(26) Rabin’s algorithm. Strong probable primes.
(27) Pollard’s $\rho$-method.
(28) Pollard’s $p - 1$ method.

Here are a few extra practice problems:

2. Practice problems

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

**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 $\sum_{i<j} a_i a_j$.

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

**Problem 4.** Solve the congruence $x^2 \equiv 17 \pmod{64}$. 
Problem 5. Find all integers \( x \) satisfying \( x \equiv 2 \) (mod 3), \( x \equiv 3 \) (mod 4), \( x \equiv 4 \) (mod 5), \( x \equiv 5 \) (mod 6).

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Historical reference: Prime numbers of the form \( M_p = 2^p - 1 \) where \( p \) is a prime are called Mersenne primes.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
\[
M_{57,885,161} = 2^{57,885,161} - 1.
\]

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Historical reference: Euclid observed that if \( p = 2^n - 1 \) is a Mersenne prime, then \( 2^{n-1}n \) is perfect.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

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 \( p \).

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

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