Review for Test 1.

I will be referring to the homeworks on the class web page. I have made some corrections and additions to these so the numbering may differ from what you have last down loaded. So you are should refer to the current versions when something like "See Theorem 3 on Homework 4" you should look at the current versions.

Since the last test the main topics we have covered are linear Diophantine equations, and the theory of congruences. So you should definitely know the statement of Theorem 1 on Homework 5 about when the linear Diophantine equation

$$ax + bx = c$$

is solvable and what the general solution is. You will definitely have to solve at least one of these equation, so know how to use the Euclidean algorithm to do this.

Sample Problem 1. Use Bézout's to show that if $\gcd(a, b) \mid c$, then $ax+by = c$ has solutions in integers. □

Sample Problem 2. For the integers $a = 126$ and $b = 368$ find integers x and y such that

$$ax + by = \gcd(a, b)$$

by use of the Euclidean algorithm. □

Sample Problem 3. Find the general solution to the following Diophantine equations.

(a) $68x + 46y = 60$
(b) $23572x + 780974y = 333$
(c) $68x - 46y = 60$ □

Sample Problem 4. How many integer solutions are there to

$$4x + 5y = 301$$

with $x, y \geq 0$? □

Sample Problem 5. Find the general solution to the Diophantine equation

$$x + 2y + 3z = 7.$$

□

You should know the definition of $a \equiv b \mod n$ and how to prove the basic facts about congruences. Thus you know how to prove Propositions 1–5 and Theorem 6 on Homework 6. We also talked about casting out nines.

Sample Problem 6. Let n be a base 10 integer such that the last (that is ones place) is 5 and the sum of the digits is 18. Show n is divisible by 45. □

We have know how to solve linear congruences such as

$$ax \equiv b \mod n$$

by reducing this to the linear Diophantine equation

$$ax + ny = b.$$

So you should be able to do problems such as Problem 14 on Homework 6.

Know the definition of $\widehat{a}$ is the inverse of a mod n and know the proof of Proposition 16 on Homework 6 compute inverses mod n (as in Problem 16 on Homework 6). Related to this would be to know how to prove Proposition 18 on Homework 6.

The next topic was the Chinese Remainder Theorem. Be able to solve problems such as Problems 21 and 23 on Homework 6.

Most recently we have proven Fermat's Little theorem and Euler's theorem. You should know the statement of both of these and how to apply them to problems such as Problems 5 on Homework 7. Related to one of our proofs of Fermat's Theorem was the result that the binomial coefficients $\binom{p}{k}$ are divisible by p when p is a prime and $1 \leq k \leq p-1$. You should be able to prove this and use it to show that

$$(x+y)^p \equiv x^p + y^p \mod p.$$

And of course there will be the usual surprise mystery questions.