Review for Test 3.

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.

Just after the last test we proved Wilson's theorem, which is that if p is prime, then $(p-1)! \equiv -1 \mod p$. And we just proved the converse of this, that if $(n-1)! \equiv -1 \mod n$, then n is prime.

A main topic has been the ***Euler phi function***, ϕ. Recall that if we set

$$U(n) = \{k : 1 \leq k \leq n, \gcd(k,n) = 1\}$$

then

$$\phi(n) = \#U(n).$$

This function has many wonderful properties. Here are some examples.

Theorem. *If* $\gcd(m,n) = 1$*, then* $\phi(mn) = \phi(m)\phi(n)$. □

Theorem. *For any positive integer* n

$$n = \sum_{d|n} \phi(d).$$

□

Proposition. *If* p *is a prime, then for any positive integers* k

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

Sample Problem 1. (a) If n is n is divisible by the prime p, then $(p-1) \mid \phi(n)$.

(b) More generally if $p^k \mid n$, then $p^{k-1}(p-1) \mid n$.

Proof of (b). p^ℓ be the latest power of p that divides n. Then $k \leq \ell$ and we have $n = p^\ell m$ where m is an integers with $\gcd(p^\ell, m) = 1$. Then

$$\phi(n) = \phi(p^\ell m) = \phi(p^\ell)\phi(m) = p^{\ell-1}(p-1)\phi(m)$$

and this is divisible by $p^{k-1}(p-1)$. □

Sample Problem 2. Find all solutions to $\phi(n) = 4$. *Answer:* $n = 5, 10, 12, 8$. □

Sample Problem 3. If n is divisible by at least 2 distinct odd primes, then $n\ \phi(n)$ is divisible by 4.

Proof. If n is divisible by p and q, odd primes with $p \neq q$, then $\phi(n)$ will have a factor of $(p-1)(q-1)$ and as $(p-1)$ and $(q-1)$ are both even, $\phi(n)$ will have a factor of 4. □

You should review the homework on Pythagorean triples and know the definitions and how to find the rational points on a quadratic curve.

Sample Problem 4. Find all Pythagorean triangles with their area three times their perimeter. *Answer:* $(a, b, c) = (13, 84, 85), (16, 30, 34), (21, 20, 29), (48, 14, 50)$. □

You should know Pick's theorem:

Theorem. *If P is a lattice polygon and I is the number of interior points of P, B the number of boundary points, then the area of P is*

$$A = B + \frac{1}{2}I - 1.$$

And you should know the both statements of Farey's theorem, see the homework on Pick's theorem and Farey's theorem.

Most recently we have been looking at the order of elements in $\mathbb{Z}_n$.

I have put up a homework *The order of elements modulo n* on the class web page. You should know the following off of it:

- Definition 5 (the order of an element modulo n)
- The statement and proof of Proposition 6.
- Definition 8 (the definition of a Primitive element)
- The statement of Proposition 9
- (Important) The Statement of Theorem 12 (Gauss' Theorem on the existence of a primitive element.)