Notes on number theory from 1/25/19
(Let me know if you have questions)

Math 417
1/28/19

1. Let $\mathbb{N} = \{1, 2, \ldots\}$ denote the set of natural numbers. For $n \in \mathbb{N}$, $n \geq 2$
n is <u>prime</u> if $n = ab$, $a, b \in \mathbb{N} \Rightarrow a = 1$ or $b = 1$. Put another way, if n is prime, $d \in \mathbb{N}$ and $d \mid n$, then $d = 1$ or $d = n$.

2. Suppose p is prime, $a \in \mathbb{N}$ and $g = \gcd(a, p)$. Then $g \mid p$ so $g = 1$ or $g = p$. That is: either $p \mid a$ or a is relatively prime to p.

3. Facts (well-known and often covered in 347): Every integer $n \geq 2$ can be written in a <u>unique</u> way as

$$n = p_1^{a_1} \cdots p_r^{a_r}, \text{ where } \begin{matrix} p_1 < p_2 < \ldots < p_r & p_j \text{ prime} \\ a_1, \ldots, a_r \in \mathbb{N} \end{matrix}$$

4. We use the notation $\nu_p(n)$ to denote the <u>power</u> of a prime p that divides n. For example, if $n = 345 = 3 \cdot 5 \cdot 23$ Then $\nu_3(345) = 1$, $\nu_5(345) = 1$, $\nu_{23}(345) = 1$, $\nu_2(345) = 0 = \nu_7(345)$, etc.

In this notation $n = 2^{\nu_2(n)} \cdot 3^{\nu_3(n)} \cdot 5^{\nu_5(n)} \cdots\cdots$ $\boxed{\text{Always. } \nu_p(1) = 0}$

5. By the usual laws of algebra and the unique representation (often called the Fundamental Theorem of Arithmetic) we observe that

$$\nu_p(mn) = \nu_p(m) + \nu_p(n)$$

Eg. $(2^3 \cdot 3 \cdot 7) \cdot (2^2 \cdot 5^2 \cdot 7) = 2^5 \cdot 3 \cdot 5^2 \cdot 7^2 \Rightarrow \nu_2(2^3 \cdot 3 \cdot 7) = 3$, $\nu_2(2^2 5^2 7) = 2$
$\nu_2(2^5 \cdot 3 \cdot 5^2 \cdot 7^2) = 5$, etc.

6. It follows from (5) that $a \mid b \Leftrightarrow \nu_p(a) \leq \nu_p(b)$ for <u>all</u> primes p.

7. Suppose $m = p_1^{a_1} \cdots p_r^{a_r}$, $n = p_1^{b_1} \cdots p_r^{b_r}$, where $a_i \ge 0, b_i \ge 0$
(I allow here $a_i = 0$ if a prime divides n and not b, etc.)
If
$q = p_1^{c_1} \cdots p_r^{c_r}$, Then $q \mid m$ and $q \mid n$ if and only if
$c_i \le a_i$ and $c_i \le b_i$ for all i. That is,
$q \mid m, n \Leftrightarrow c_i \le \min(a_i, b_i)$, $1 \le i \le m$. Put another way
$\gcd(m,n) = p_1^{\min(a_1,b_1)} \cdots p_r^{\min(a_r,b_r)}$, or put another way:
$\nu_p(\gcd(m,n)) = \min(\nu_p(m), \nu_p(n))$.

8. Theorem: If $\gcd(a,c)=1$ and $\gcd(b,c)=1$, Then $\gcd(ab,c)=1$.
Proof 1:
Note That $\gcd(a,c)=1$ means That any prime That divides c cannot divide a, and $\gcd(b,c)=1$ means That any prime That divides c cannot divide b. If p is a prime dividing ab, Then $p \mid a$ or $p \mid b$, so p can't be a prime dividing c.

Proof 2 (Non-conceptual)
There exist integers r, s so That $ar + cs = 1$ and integers t, u so That $bt + cu = 1$. So...
$ar + cs = 1 \Rightarrow arb + csb = b$ and $bt + cu = 1 \Rightarrow (arb + csb)t + cu = 1$
$\Rightarrow arbt + csbt + cu = 1 \Rightarrow (ab)(rt) + c(sbt + u) = 1$.

9. The Euler phi function $\phi(n)$ is defined to be The number of integers a, $0 < a < n$ for which $\gcd(a,n)=1$.
Eg. $\phi(4) = 2$: $\gcd(1,4) = \gcd(\,,4) = 1$, $\gcd(2,4) = 2 > 1$
$\phi(8) = 4$: $\gcd(1,8) = \gcd(3,8) = \gcd(5,8) = \gcd(7,8) = 1$
$\phi(14) = 6$: $\gcd(a,14) = 1$ for $a = 1, 3, 5, 9, 11, 13$

10. Suppose p is prime and $m \geq 1$. We can compute $\phi(p^m)$ directly. How can it be that $\gcd(a, p^m) > 1$? Then $g \mid p^m$, which means that g is a power of p. Thus, $\gcd(a, p^m) > 1 \iff p \mid g$.

How many multiples of p are there $< p^m$?
$a = p \cdot b \quad 0 \leq a < p^m \iff 0 \leq pb < p^m \iff 0 \leq b < p^{m-1}$
So there are p^{m-1} multiples and $\phi(p^m) = p^m - p^{m-1}$.

We have $4 = 2^2$, $\phi(4) = 2^2 - 2^1$; $8 = 2^3$, $\phi(8) = 2^3 - 2^2$ from the last page. Here's another one: $9 = 3^2$.
$a = \cancel{0}, 1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, 8$. (I've crossed out the multiples of $3 < 9$, so $\phi(9) = 3^2 - 3 = 6$.

11. Suppose $\gcd(m, n) = 1$. We claim that $\phi(mn) = \phi(m)\phi(n)$. This is a sketch of the proof. We use the Chinese Remainder Theorem, and the fact that $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$ $\iff \gcd(a, mn) = 1$. (Why is this fact true? In one direction, it's #8 with the letters changed. In the other, if $\gcd(a, mn) = 1$ then a has no primes in common with mn, and so automatically none in common with m or n.) Rather than a proof, I will illustrate it with $m = 5$, $n = 6$, $mn = 30$

	$a \equiv 0 \bmod 6$	$a \equiv 1 \bmod 6$	$a \equiv 2 \bmod 6$	$a \equiv 3 \bmod 6$	$a \equiv 4 \bmod 6$	$a \equiv 5 \bmod 6$
$a \equiv 0 \bmod 5$	~~0~~	~~25~~	~~20~~	~~15~~	~~10~~	~~5~~
$a \equiv 1 \bmod 5$	~~6~~	1	~~26~~	~~21~~	~~16~~	11
$a \equiv 2 \bmod 5$	~~12~~	7	~~2~~	~~27~~	~~22~~	17
$a \equiv 3 \bmod 5$	~~18~~	13	~~8~~	~~3~~	~~28~~	23
$a \equiv 4 \bmod$	~~24~~	19	~~14~~	~~9~~	~~4~~	29

I have xed common factors of 5 and common factors of 6 (diagonally)
What's left is: 1, 7, 13, 19, 11, 17, 23, 29: $\phi(30) = \phi(5)\phi(6) = 4 \cdot 2 = 8$