Math 312, lecture 7

(1) Test 1
(2) Unique factorization
(3) Linear equations

On course website now: sample exam front pages (grab yours?)
During test set your paper by changing "Test 0" to "Test 1".

(2) Unique factorization.
Last time: (1) Primality: plab iff pla or plb.
(2) Every positive integer is a product of primes, uniquely up to reordering factors.
\[ 48 = 2 \cdot 74 = 2^3 \cdot 3^4. \]
(for non-zero integers there is a possible sign)
New notation: \( \Pi \) is to "product" as \( \Sigma \) is to "sum"!

Example: \( n! = \prod_{k=1}^n k \).

Unique factorization: integer \( n \) is determined by saying, for each prime \( p \), how many times \( p \) divides \( n \).

\[ 198 = 2^2 \cdot 3^2 \cdot 11^1 \cdot 31^1 \cdot 37 \cdot 41 \cdots \]

2 twice, other primes 37 once, 0 times.

For a general integer write:

\[ n = 3 \cdot \prod_{p} \frac{e_p}{p} \]

how many times \( p \) appears

These products make sense because only finitely many \( e_p \) are non-zero.
Divisors of \( n \): Those \( m \) st

\[
m = \delta \cdot \prod p^{e_p}
\]

with \( e_p \leq f_p \) for all \( p \)

(divisors of \( 148: 2^2 \cdot 37 \), \( 0 \leq a \leq 2 \))

Cor.: if \( n = \delta \cdot \prod p^{e_p} \)

\[
m = \delta \cdot \prod p^{f_p}
\]

Then common divisors are \( \prod p^{g_p} \)

where \( 0 \leq g_p \leq \min\{e_p, f_p\} \)

(divisors of \( 148 \) contained at most twice,

" " 6 " 2 " once

common divisors " " " once)

\[\Rightarrow \gcd (n, m) = \prod p^{\min\{e_p, f_p\}}\]

\((148, 6) = (2^2 \cdot 3 \cdot 37, 2^1 \cdot 3 \cdot 37^0)\]

\[= 2^1 \cdot 3^0 \cdot 37^0 = 2\]

(choose smaller exponent)
For multiples: \( m/n \) if exponents of \( m \) are smaller, then
\[
\left[ n, m \right] = \prod_p \max \left\{ e_p, f_p \right\}
\]

Eg.
\[
\left[ 148, 6 \right] = \left[ 2^2 \cdot 3 \cdot 37^1, 2^1 \cdot 3 \cdot 37^0 \right] = 2^2 \cdot 3 \cdot 37^1
\]

\[\text{Corr. } \left[ n, m \right] = \left( \prod_p \min \left\{ e_p, f_p \right\} \right) \left( \prod_p \max \left\{ e_p, f_p \right\} \right)\]
\[
= \prod_p \min \left\{ e_p, f_p \right\} + \max \left\{ e_p, f_p \right\} = \prod_p e_p + f_p
\]
\[
= \left( \prod_p e_p \right) \cdot \left( \prod_p f_p \right) = \ln(nm).
\]

Observation: proof is easier than the previous one using Bezout’s thm.

Computationally this is hard.
More applications: PS 3: \( h^k = \prod \pi_p^l \)

(n is a square iff all exponents even)

\( \Rightarrow 2 \) is not a square in \( \mathbb{Z} \), even in \( \mathbb{Q} \)

(\( \sqrt{2} \) is irrational)

More: PS 2: want to solve an equation like \( y^2 = x^3 + 1 \) in \( \mathbb{Z} \)

can write this as \( 8y^2 - 1 = x^3 \)

\( \Rightarrow \) \((y-1)(y+1) = x^3 \)

then \( y-1, y+1 \) are relatively primes: \((y+1, y-1) = (y+1, 2) \in \{1, 2\}\)

check exponent by exponent, up to factor that \( y-1, y+1 \) both cubes (one of 2)

only \( 41, -1 \) are cubes that differ by \( 2 \) \( \Rightarrow \) (only solutions are \( 1^2 = 0^3 + 1 \), \( 3^2 = 2^3 + 1 \)).
(notes: find more gcd calculations:
Formal Mersenne numbers:
\[ \begin{align*}
2^n - 1, & \quad 2^n + 1.
\end{align*} \]
(Asides on counting primes)

Change of topics:

Def: A Diophantine equation is an equation to be solved by integers
(Diophantus of Alexandria wrote a book on the topic)

The prototypical point of number theory.
(looked about at \( x^2 = 2 \)
\[ y^2 = x^3 + 1 \])

Like any other kind of equations, want to address:

1. Are there any solutions?
2. How many, if they exist?
3. How do we find them?
Like any other equation, "solving" an equation means doing 2 things:

1. Write down a list of "solutions".
2. Show that every solution appears in the list.

"If x is a solution then ..." on the list.

(2) Show that every member of the list is a solution.

"Plug in to the equation.

In practice start at step (1), use step (2) to determine the correct list.

Example: Let's solve \( x = 5 \).

If \( x = 5 \) then \( 0 \cdot x = 0 \cdot 5 \)

But any \( x \) satisfies \( 0 \cdot x \leq 0 \)

So all \( x \) solve equation?

Exampleless

(1) Linear equation in one variable:
\[ 2x = 6, \quad 2x = 7 \]
("divisibility")

2) Linear equations in several variables
   (next topic) \(6x + 8y = 7\)
   (gcd, Bezout's theorem play a big role)

3) Non-linear equations:
   \(x^2 = 2\) (Irrationality of \(\sqrt{2}\))
   \(x^2 + y^2 = z^2\) ("Pythagorean triples")

   \(p23: x^p + y^p = z^p\) (Fermat's equation)
   \(p23\) has no solutions unless one of \(x, y, z\) is zero.

   \(p = 2, 3\) Fermat
   \(p = 3\) Euler

   general \(p\) due to Ribet, Wiles

Taylor-Wiles (BCDTS)