MATHEMATICAL ENRICHMENT CLASS / OLYMPIAD TRAINING

9 MARCH 2019 PROFESSOR GARY MCGUIRE

NUMBER THEORY

$\mathbb{Z}$ = the integers = $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$\mathbb{N}$ = positive integers = $\{1, 2, 3, \ldots\}$

$\mathbb{Q}$ = rational numbers = $\left\{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\right\}$

$\frac{2}{3}$, $\frac{314}{1000}$, $\frac{22}{7}$

Diophantine equation – solutions in $\mathbb{Z}$, or $\mathbb{Q}$

e.g. $x^2 + y^2 = z^2$ $\quad$ $x^3 + y^3 = z^3$

3 4 5

Let $d, n \in \mathbb{Z}$

We say "d divides n" (written $d|n$) if there exists $m \in \mathbb{Z}$ such that $n = md$ e.g. $3|51$

Theorem 1 If $d|n$ and $d|r$ then $d|(an+br)$ for any integers a, b

e.g. d divides $n+r$, $n-r$, $n+2r$, $3n+5r$

proof If $d|n$ then $n = md$, for some $m \in \mathbb{Z}$

If $d|r$ then $r = sd$, for some $s \in \mathbb{Z}$

Then $an+br = amd + bsd = d(\underbrace{am+bs}_{\text{This} \in \mathbb{Z}})$. So $d|(an+br)$.

A prime number is an integer > 1 with no divisors other than itself and 1

e.g. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ...

Unsolved question: are there infinitely many pairs of primes?

11,13 17,19 29,31 41,43

Theorem 2 Every integer is divisible by a prime.

proof By complete / strong induction.

If n is prime, done.

If n is not prime, let $n = ab$ where $1 < a < n$, $1 < b < n$.

By assumption, a is divisible by a prime.

So n is divisible by this prime.

Fundamental Theorem of Arithmetic: Every positive integer > 1 can be written as a product of prime numbers in a unique way, up to order.

(proof omitted).

e.g. $24 = 2 \cdot 2 \cdot 2 \cdot 3$

$30 = 2 \cdot 3 \cdot 5$

we usually write the prime factorization of n as

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where $p_1, \ldots, p_r$ are distinct primes and each $k_i \geq 1$, $k_i \in \mathbb{Z}$

Every divisor of n has the form $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $a_i \leq k_i$

Remark $\tau(n)$ = number of divisors of n

$$= (k_1+1)(k_2+1)\cdots(k_r+1)$$

e.g. $\tau(24) = (3+1)(1+1) = 4 \cdot 2 = 8$

$2^0 3^0 = 1$
$2^1 3^0 = 2$
$2^2 3^0 = 4$
$2^3 3^0 = 8$
$2^0 3^1 = 3$
$2^1 3^1 = 6$
$2^2 3^1 = 12$
$2^3 3^1 = 24$

$\sigma(n)$ = sum of the divisors of n

$$= (1 + p_1 + p_1^2 + \cdots + p_1^{k_1})(1 + p_2 + p_2^2 + \cdots + p_2^{k_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r})$$

e.g. $\sigma(24) = (1+2+2^2+2^3)(1+3)$

$= (15)(4) = 60$

n is **perfect** if $\sigma(n) = 2n$ e.g. $\sigma(6) = 1+2+3+6 = 12$

6 is perfect.

Unsolved problem: are there any odd perfect numbers?

Study $\sigma(n)$ and $\tau(n)$ later.

Theorem 3 (Euclid) There are infinitely many prime numbers.

proof Suppose not. Let $p_1, p_2, \ldots, p_r$ be all the prime numbers. Let $N = p_1 p_2 \cdots p_r + 1$

By Theorem 2, N is divisible by a prime. Call it p.

If p_i divides N then p_i divides $N - p_1 p_2 \cdots p_r$ by Theorem 1, so the prime p is not p_i

But then p_i divides 1, impossible. Contradiction.

---

odd numbers have the form

$4n+1$: 5, 9, 13, 17, 21, 25, 29, 33, ---

$4n+3$ 7, 11, 15, 19, 23, 27, 31, 35, -----

Congruences Fix an integer $m > 1$.

Say $a \equiv b \pmod m$ if $m \mid (a-b)$.

"a is congruent to b modulo m" e.g. $1 \equiv 3 \pmod 2$

$59 \equiv 44 \pmod 5$

numbers of the form $4n+1$ are all $\equiv 1 \pmod 4$ $25 \equiv 1 \pmod 4$

" " " " $4n+3$ " " $\equiv 3 \pmod 4$ $35 \equiv 3 \pmod 4$

property if $a \equiv x \pmod m$ and $b \equiv y \pmod m$

then $ab \equiv xy \pmod m$. $(a^2 \equiv x^2 \bmod m)$

e.g. $(25)(35) \equiv (1)(3) \pmod 4$

$\equiv 3 \pmod 4$

e.g. $2^3 \equiv 1 \pmod 7$

square both sides $2^6 \equiv 1 \pmod 7$

keep squaring - - - - . or raise to any power eg. 100

$2^{600} \equiv 1 \pmod 7$

7 divides $2^{600} - 1$

Divisibility by 3 Let $n = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ where $0 \le a_i \le 9$

e.g. $437 = 4 \cdot 10^2 + 3 \cdot 10 + 7$

$10 \equiv 1 \pmod 3$. So $10^k \equiv 1^k \equiv 1 \pmod 3$ any k

Therefore $n \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3$

So $n \equiv 0 \pmod 3$ if and only if $a_n + a_{n-1} + \cdots + a_1 + a_0 \equiv 0 \pmod 3$

e.g. 432 is divisible by 3 because $4+3+2 = 9$ is divisible by 3.

Let $n \equiv 1 \pmod 4$ and $m \equiv 1 \pmod 4$.

Then $nm \equiv 1 \pmod 4$. (*)

Theorem 4 There are infinitely many primes $\equiv 3 \pmod 4$.

proof Suppose not. Let $p_1, p_2, \ldots, p_r$ be all the primes $\equiv 3 \pmod 4$ not counting 3.

Let $N = 4 p_1 p_2 \cdots p_r + 3$.

If all prime divisors of N are $\equiv 1 \bmod 4$, then

$N \equiv 1 \pmod 4$ by (*).

But $N \equiv 3 \pmod 4$. So N must have a prime divisor that is $\equiv 3 \pmod 4$.

This cannot be any of $p_1, p_2, \ldots, p_r$. (otherwise they would divide 3)

So there is another prime $\equiv 3 \bmod 4$. Contradiction.

Fermat's Little Theorem Let p be prime.

Then $a^{p-1} \equiv 1 \pmod p$ for any $a \in \mathbb{Z}$ not divisible by p.

e.g. $2^{100} \equiv 1 \pmod{101}$.

$3^{100} \equiv 1 \pmod{101}$