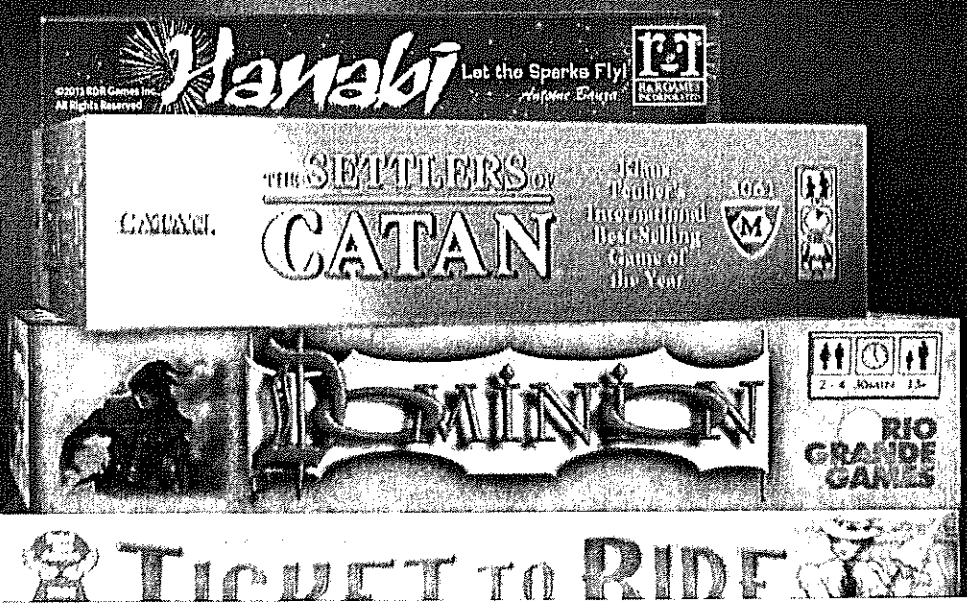
Starts 6:30pm

Thursday October 15th in the C&D

Free food and drinks

Games Night with Profs



MathSoc

Theorem (Euclid) There exists infinitely many primes.

Pf: Assume towards a contradiction that $\exists$ finitely many primes

$$p_1, p_2, \dots p_n.$$

Consider $N = \prod_{i=1}^{n} p_i + 1$. By FTArithmetic, N can be written as a product of primes. In particular, $\exists$ a prime $p \mid N$. So $p = p_i$ for some $1 \le i \le n$. As $p \mid N$ & $p \mid \prod_{i=1}^{n} p_i$, we conclude by DK, $p \mid N - \prod_{i=1}^{n} p_i = 1$ #.

Gap in FT Arithmetic

Need: $p \mid \prod_{i=1}^{k} n_i$ for $n_1, n_2, \ldots n_k \in \mathbb{Z}$ then $p \mid n_i$ for some $1 \leq i \leq k$.

To prove this, need Euclid's Lemma

p is a prime $\wedge\, p \mid ab \Rightarrow p \mid a \vee p \mid b$.

To prove this we need Bézout's Lemma and gcds.

// GCD (Greatest Common Divisor)

Divisors of 84:

$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 7, \pm 12, \pm 14, \pm 21, \pm 28, \pm 42, \pm 84$

Divisors of 120:

$\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 8, \pm 10, \pm 12, \pm 15, \pm 20, \pm 24,$
$\pm 30, \pm 40, \pm 60, \pm 120.$

So the greatest common divisor of 84 and 120 is 12.

Def'n: The greatest common divisor of integers a and b with $a \neq 0$ or $b \neq 0$ is an integer $d > 0$ such that

(i) $d \mid a \wedge d \mid b$

(ii) If $c \mid a \wedge c \mid b$ then $c \leq d$.

We write $d = \gcd(a, b)$.

Notes:

- $\gcd(a, a) = |a| = \gcd(a, 0)$
- Define $\gcd(0, 0) = 0$. Note $\gcd(a, b) = 0 \iff a = b = 0$.
- Ex: $\gcd(a, b) = \gcd(b, a)$

Prove that $\gcd(3a + b, a) = \gcd(a, b)$ using the definition directly.

d e

So $d \mid 3a+b$ $\wedge$ $d \mid a$. Then

DIC $\Rightarrow$ $d \mid (3a+b) - 3a = b$

Since e is the maximal divisor of a and b, $d \leq e$.

So $e \mid a$ and $e \mid b$. Then

DIC $\Rightarrow$ $e \mid 3a + b$. Since d is maximal, $e \leq d$.

Hence $d = e$. ∎

Claim: $\gcd(a,b)$ exists.

Pf: Suppose $a \neq 0$ or $b \neq 0$.
Clearly $1 \mid a$ and $1 \mid b$.
So a divisor exists.

There is a greatest common divisor
Since $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$
so $\gcd(a,b) \leq \min\{|a|, |b|\}$ by BBD.
Thus, $1 \leq \gcd(a,b) \leq \min\{|a|, |b|\}$. ☐

Claim: $\gcd(a,b)$ is unique.

Pf: Suppose d and e are both the greatest common divisor of a and b.
Then $d \mid a \wedge d \mid b$ so since e is maximal $d \leq e$. Similarly $e \leq d$. Hence $d = e$. ☐

Let $a, b \in \mathbb{N}$.

Claim: If $n = ab$ then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Pf: Suppose $n = ab$ and $a > \sqrt{n}$.

$ab > b\sqrt{n}$

$n > b\sqrt{n}$

$\sqrt{n} > b \Rightarrow b \leq \sqrt{n}$ ▶.

GCD with Remainder (GCDwR)

If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$ then $\gcd(a,b) = \gcd(b,r)$

Ex: $\gcd(72, 40) = 8$

Now, $72 = 40(1) + 32$

So GCDwR says $\gcd(72, 40) = \gcd(40, 32$

Again: $40 = 32(1) + 8$ so

$\gcd(40, 32) = \gcd(32, 8)$

Pf of GCDWR:

If $a=b=0$, then $r = a - bq = 0$

So $\gcd(a,b) = 0 = \gcd(b,r)$

If $a \neq 0$ or $b \neq 0$ . . .