THE MATH BEHIND ISBN NUMBERS[1]

Math 300 Spring 2004

For any integers m, n, d, we say $m \equiv n \bmod d$ if d divides $m - n$ evenly. That is, $(m - n) = dq$ for some integer q. A non-negative integer $p \neq 1$ is prime if is divisible only by itself and 1. We assume the 'division algorithm': for any integer a and positive integer d there are integers q and r with $0 \leq r < d$ such that $a = dq + r$.

Lemma 0.1 *For any d if $m \not\equiv 0 \bmod d$ then for any a, $a \not\equiv a + m \bmod d$.*

Proof. If $a \equiv a + m \bmod d$, d divides $a - (a + m)$ evenly, that is a divides m evenly so $m \equiv 0 \bmod d$.

Definition 0.2 *An ideal I is a set of integers closed under addition and subtraction. (Equivalently, if $a \in I$ and n is an integer then $na \in I$.)*

Thus the smallest ideal containing two positive integers a, b is the set of all linear combinations: $xa + yb$ with x, y integers. We call this the ideal generated by a and b.

Definition 0.3 *The* greatest common divisor *of a and b is the largest positive integer that evenly divides both a and b.*

Theorem 0.4 *If a and b are positive integers the least number in the ideal I generated by a and b is the greatest common divisor of a and b.*

Proof. Let d be the smallest positive number in I. Suppose for contradiction that d does not divide a. So $a = dq + r$ with $0 < r < d$. But d also equals $xa + by$. So

$$r = a - (xa + by)d = (x - 1)a + by.$$

This contradicts the assumption that d is the smallest positive number in I. For similar reasons d divides a. Any number which divides both a and b divides any linear combination of them, in particular, d. Thus, d is the greatest common divisor.

Lemma 0.5 *If a prime p divides a product ab, it must divide one of the factors.*

Proof. If p does not divide a then the greatest common divisor of a and p is 1 so by Lemma 0.4 for some x, y, $xp + ya = 1$. So $xpb + yab = b$. Since p divides ab, we conclude by Lemma 0.1, that p divides b, as required.

[1] PSee Number Theory by Hardy and Wright

1 Number of Primes

This page is an entertaining proof that there are infinitely many primes. It is purely for you amusement and is not needed for the assignment.

As a geometric series, for any prime p:

$$\frac{1}{1-\frac{1}{p}} = \Sigma_{n=1}^{n=\infty} \frac{1}{p^n}.$$

So

$$\Pi_p \frac{1}{1-\frac{1}{p}} = \Pi_p \Sigma_{n=1}^{n=\infty} \frac{1}{p^n}.$$

where the product is taken over all primes p. Note that since every n is uniquely written as a product to primes the right hand side equals

$$\Sigma_{n=1}^{n=\infty} \frac{1}{n}.$$

Since the harmonic series diverges the right hand side is infinite. But if there are only finitely many primes the left hand side is finite.