Math 445 Number Theory

August 27, 2004

An integer $p \geq 2$ is *prime* if the only $a|p$ are ± 1 and $\pm p$.

Fundamental Theorem of Arithmetic: Every integer is a product of primes, unique up to re-ordering.

Because: if there is an n which isn't, then there is a *smallest* one; then it isn't prime (else $n = p$ is the product), so $n = ab$ with $1 < a, b < n$, so each is a product of primes, so n is a product of their products, a contradiction.

Uniqueness: need *If p is prime and $p|a_1 \cdots a_n$, then $p|a_i$ for some i.* Then if $n = p_1 \cdots p_k = q_1 \cdots q_l$, then $p_1|q_i$ for some i, so $p_1 = q_i$, so $p_2 \cdots p_k = q_1 \cdots q_{i-1}q_{i+1} \cdots q_l$. Continuing, we can pair all the p's with q's. [Better? If not always unique, there is a *smallest* number without unique factorization; structure proof as before.]

Completely factoring a number a la FTA has two parts; find factors, and decide when they are prime. But how do you decide that a number $N \geq 2$ is prime?

(1) $a|b$ implies $|a| \leq |b|$. So check that no $1 < a < N$ divides N .

(2) $N = ab$ implies $|a| \leq \sqrt{|N|}$ or $|b| \leq \sqrt{|N|}$. So check that no $1 < a \leq \sqrt{N}$ divides N .

(3) A prime factorization $N = p_1 \cdots p_k$ with $p_1 \leq p_2 \leq \ldots \leq p_k$ is unique. Then (if $k \geq 2$, i.e., N is not prime)

$$p_1^2 \leq p_1^k = p_1 \cdots p_1 \leq p_1 \cdots p_k = N, \text{ so } p_1 \leq \sqrt{N}$$

So check that no *prime* p, $1 < p \leq \sqrt{N}$ divides N .

Almost every other primality (or factoring) test involves *Fermat's Little Theorem.*

Typo on Introduction sheet:

(2) $d = \gcd(a, b)$ is the smallest *positive* number that can be written as $d = ax + by$ with $x, y \in \mathbb{Z}$. (**Not** with $a, b \in \mathbb{Z}$ ...) There is a similar typo in property (4).