414 = Lecture 2: Prime Factorization

Prop: Suppose $a, b \in \mathbb{Z}$, $b \neq 0$.
Then there exists unique $q, r \in \mathbb{Z}$ s.t.

$$a = bq + r, \quad 0 \leq r < |b|.$$

‖ something very special about $\mathbb{Z}$.

Remark: compute q, r via long division

Proof: WLOG assume $a, b > 0$.

Existence:
$0 \in Q = \{ n \geq 0 : a - bn \geq 0 \} \neq \emptyset$. is bounded, since $n \leq \frac{a}{b}$.

Let $q = \max(Q)$.

Then $r = a - bq < b$, so $a = bq + r$ and $0 \leq r < b$, as required!

Uniqueness:

Suppose $a = bq' + r'$ with $0 \leq r' < b$.

$a - bq' \geq 0 \Rightarrow q' \in Q$ so $q' \leq q$, say $q' = q - m$ for $m \geq 0$.

$m \geq 1 \Rightarrow r' = a - bq' = a - b(q-m) = a - bq + bm = r + bm \geq b$, ⚡.

So $m = 0 \Rightarrow q = q' \Rightarrow r = r'$. □

How to compute gcd's without factoring:

$\gcd(a, b)$. Say $a \geq b > 0$.

$$a = bq + r$$

Observe: $\gcd(a,b) = \gcd(b,r)$. And (b, r) are much smaller!

$d \mid a$ & $d \mid b \Leftrightarrow d \mid r = a - bq$ & $d \mid b$ ✓

Example: $\gcd(2010, 2007)$.

$$2010 = 2007 \cdot 1 + 3$$
$$2007 = 3 \cdot 669 + 0$$

$$\gcd(2010, 2007) = \gcd(2007, 3) = \gcd(3, 0) = 3.$$

$$3 \overline{)2007}\ 669,\ 18,\ 20,\ 18,\ 27$$

Example: $\gcd(2261, 1275)$

$$2261 = 1275 \times 1 + 986$$
$$1275 = 986 \times 1 + 289$$
$$986 = 289 \times 3 + 119$$
$$289 = 119 \times 2 + 51$$
$$119 = 51 \times 2 + 17$$

$$\gcd(2261, 1275) = \gcd(1275, 986) = \gcd(986, 289) = \gcd(289, 119) = \gcd(119, 51) = \gcd(51, 17) = 17. \checkmark$$

Sage: type "gcd(2261, 1275)".

That's it. Inputs can have
- arbitrarily many digits.
- actual algorithm is complicated and state of the art.

Recall: Current goal is to prove FTA.
Need: $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Lemma: $\gcd(an, bn) = \gcd(a, b)\,|n|$.

Proof: "At every step of the above algorithm, everything is multiplied through by n."

$$an = bn \cdot q + rn.$$

$$\gcd(an, bn) = \gcd(bn, rn)$$

$$\gcd(\gcd(a,b) \cdot n, 0) = \gcd(a,b) \cdot |n|.$$

Lemma: $n \mid a$ and $n \mid b \Rightarrow n \mid \gcd(a,b)$.

Proof: $nc_1 = a \qquad nc_2 = b$

$\gcd(a,b) = \gcd(c_1 n, c_2 n) = \gcd(c_1, c_2) \cdot |n|$ ∎

$\Rightarrow n \mid \gcd(a,b)$.

Prop: p prime, $a, b \in \mathbb{N}$

$p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Proof: If $p \mid a$, done.

If $p \nmid a$ then $\gcd(p,a) = \max\{1\} = 1$.

$\Rightarrow \gcd(pb, ab) = b$

But $p \mid pb$ and $p \mid ab$ so by Lemma $p \mid b$. ∎

Conclusion: **Theorem:**

$$p_1 \cdots p_e = q_1 \cdots q_f$$

$$p_1 \mid q_1 \cdots q_f \Rightarrow p_1 = q_1 \text{ or } p_1 \mid q_2 \cdots q_f$$

$$\Rightarrow \cdots p_1 = q_i \text{ some } i.$$

so $p_2 \cdots p_e = q_1 \cdots \widehat{q_i} \cdots q_f$

$\vdots$

etc.

$1 = 1$. so factorization is unique!

Factoring Integers:

Exercise: If n is composite then some prime $p \mid n$ with $p \leq \sqrt{n}$.

$\rightsquigarrow$ $O(\sqrt{n})$ complexity algorithm.

O.K. if n is your soc.

BAD if n has 100 digits (say).

Sage: has some better factoring algorithms.

```
sage: factor(2010)
2 * 3 * 5 * 67
sage: factor(-, verbose=8)
sage: factor?
```

Open Problem: Is there a "fast" algorithm to factor? No one knows.

"fast" $=$ complexity $= O(f(\log(n)))$ where f is a polynomial.

P. Shor: If you can build a "quantum computer" it can factor quickly.

The RSA cryptosystem encrypts messages using assumption that factoring $p_1 p_2$ is hard. More later.

Next: the sequence of primes

2, 3, 5, 7, ...