

CS181A Notes #2 Basic Number Theory

Theorem 1. (Euclid) *There are infinitely many prime numbers.*

Proof. Suppose there are only finitely many primes, say $\{p_1, p_2, \dots, p_m\}$. Since any number is divisible by some prime, $q = p_1 p_2 \dots p_m + 1$ must be divisible by some prime, say p_j , from the list. But this implies p_j divides 1, which is a contradiction. $\square$

Exercise 1. *Extend the proof to primes of the form $4k + 3$, for a positive integer k . What about primes of the form $4k + 1$?*

Theorem 2. (Euclid's GCD algorithm)

For any integers a and b , where $a \geq b \geq 0$, we have

$$\gcd(a, b) = \begin{cases} a & \text{if } b = 0 \\ \gcd(b, a \bmod b) & \text{if } b > 0 \end{cases} \quad (1)$$

Proof. The base case is clear. We need to show that $\gcd(a, b) = \gcd(b, a \bmod b)$ for $a \geq b > 0$. Let $r = a \bmod b$. Then, $r = a - qb$, for some quotient q with $0 < r < b$. Suppose $d = \gcd(a, b)$ and $e = \gcd(b, r)$. It is clear that $d|b$ (by definition) and that $d|r$ (since r is a linear combination of a and b). Thus, $d|e$ since $e = \gcd(b, r)$. Similarly, $e|d$ given that it divides both b and r and that $a = qb + r$. Therefore, $d = e$. $\square$

Corollary 1. (Pulverizer of Aryabhata)

For any integers $a \geq b \geq 0$, where $d = \gcd(a, b)$, there are integers $x, y \in \mathbb{Z}$ so that

$$d = xa + yb.$$

Moreover, d is the smallest positive member of the set $\{xa + yb : x, y \in \mathbb{Z}\}$.

Finding Aryabhata: There is a natural way of adapting Euclid's algorithm to recursively compute the *extended* constants x and y so that $d = xa + yb$. But a simpler algorithm is the following iterative version. Given the numbers a and b , allocate two pairs of coefficients, say $\{x_1, y_1\}$ and $\{x_2, y_2\}$, so that these invariants hold:

$$a^{(k)} = x_1^{(k)} a + y_1^{(k)} b, \quad b^{(k)} = x_2^{(k)} a + y_2^{(k)} b, \quad (2)$$

where the superscript k keeps track of the k -iteration in the algorithm. The algorithm begins by setting: $x_1^{(0)} = 1$, $y_1^{(0)} = 0$ and $x_2^{(0)} = 0$, $y_2^{(0)} = 1$. The

invariant is clearly satisfied. At the end, when $b^{(K)} = 0$, note that we have $\gcd(a, b) = a^{(K)} = x_1^{(K)}a + y_1^{(K)}b$ which yields the solution. What remains is to show that we can compute the pair of coefficients moving forward. So, having (2) in hand, since $a^{(k+1)} = b^{(k)}$ we immediately have

$$x_1^{(k+1)} = x_2^{(k)}, y_1^{(k+1)} = y_2^{(k)}.$$

Furthermore, $b^{(k+1)} = a^{(k)} \pmod{b^{(k)}}$ (by definition of Euclid's algorithm). Moreover, the remainder is a linear combination of $a^{(k)}$ and $b^{(k)}$:

$$b^{(k+1)} = a^{(k)} - qb^{(k)} \tag{3}$$

$$= [x_1^{(k)}a + y_1^{(k)}b] - q[x_2^{(k)}a + y_2^{(k)}b] \tag{4}$$

$$= [x_1^{(k)} - qx_2^{(k)}]a + [y_1^{(k)} - qy_2^{(k)}]b \tag{5}$$

$$= x_2^{(k+1)}a + y_2^{(k+1)}b \tag{6}$$

Theorem 3. (Fermat's Little Theorem)

Let p be a prime number. Then, for any $a \not\equiv 0 \pmod{p}$, we have

$$a^{p-1} \equiv 1 \pmod{p}. \tag{7}$$

Proof. First, note that the map $f_a(x) \equiv ax \pmod{p}$ is a bijection, for any $a \not\equiv 0 \pmod{p}$. The claim follows by observing the following equivalent products:

$$\prod_{x \not\equiv 0} x \equiv \prod_{x \not\equiv 0} f_a(x) \equiv a^{p-1} \prod_{x \not\equiv 0} x. \tag{8}$$

The first equivalence follows since f_a is bijective whereas the second is from commutativity. Since each x has an inverse modulo p , we have proved our claim. $\square$

Exercise 2. Prove Euler-Fermat's Little Theorem. Let n be any integer. Then, for any $a \not\equiv 0 \pmod{n}$, we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

Theorem 4. (Chinese Remainder Theorem)

Let $n = pq$ where p and q are two distinct primes. Suppose that $z \equiv a \pmod{p}$ and $z \equiv b \pmod{q}$ hold simultaneously. Then, there is a unique $z \pmod{n}$ which satisfies the above two congruences.

Proof. Suppose we have two numbers α_p and α_q with the properties:

$$\alpha_p \equiv \begin{cases} 1 & (\text{mod } p) \\ 0 & (\text{mod } q) \end{cases} \quad \alpha_q \equiv \begin{cases} 0 & (\text{mod } p) \\ 1 & (\text{mod } q) \end{cases} \quad (9)$$

Then, $z = (a\alpha_p + b\alpha_q) \pmod n$ is our solution. Since $\gcd(p, q) = 1$, there are integers x and y so that $1 = xp + yq$. The proof is done by observing that $\alpha_p = yq$ and $\alpha_q = xp$ satisfy (9). $\square$

Exercise 3. *Extend the Chinese Remainder Theorem to allow pairwise relatively prime moduli and also to the case for more than two simultaneous congruences.*

Lemma 1. *Let p be a prime and suppose $p|ab$ for two integers a and b . Then, $p|a$ or $p|b$.*

Proof. If $p|a$, then we are done. Suppose p does not divide a , and thus $\gcd(p, a) = 1$. By the extended Euclidean algorithm, there are integers x and y so that $1 = xp + ya$. This shows $b = xpb + y(ab)$, whereby $p|b$ follows. $\square$

Lemma 2. *If p is prime, then the quadratic equation $x^2 \equiv 1 \pmod p$ has exactly two solutions, namely $x \equiv \pm 1 \pmod p$.*

Proof. First, we rewrite the quadratic equivalently as $x^2 - 1 \equiv 0 \pmod p$ which implies $p|(x - 1)(x + 1)$. Thus, either $p|(x - 1)$ (from which $x \equiv +1 \pmod p$ follows) or $p|(x + 1)$ (from which $x \equiv -1 \pmod p$ follows). There are no other possibilities. $\square$