

## Problem Set 5

Due: March 13

**Reading:** Chapter 8. *Number Theory* through 8.10. *Euler's Theorem*.

### Problem 1.

Extend the binary gcd procedure of Problem 8.16 to obtain a new pulverizer that uses only division by 2 and subtraction.

*Hint:* After the binary gcd procedure has factored out 2's, it starts computing the  $\gcd(a, b)$  for numbers  $a, b$  at least one of which is odd. It does this by successively updating a pair of numbers  $(x, y)$  such that  $\gcd(x, y) = \gcd(a, b)$ . Extend the procedure to find and update coefficients  $u_x, v_x, u_y, v_y$  such that

$$u_x a + v_x b = x \text{ and } u_y a + v_y b = y.$$

To see how to update the coefficients when at least one of  $a$  and  $b$  is odd and  $ua + vb$  is even, show that either  $u$  and  $v$  are both even, or else  $u - b$  and  $v + a$  are both even.

### Problem 2.

Suppose that  $p$  is a prime and  $0 < k < p$ .

(a)  $k$  is self-inverse if  $k^2 \equiv 1 \pmod{p}$ . Prove that  $k$  is self-inverse iff either  $k = 1$  or  $k = p - 1$ .

*Hint:*  $k^2 - 1 = (k - 1)(k + 1)$

(b) The English mathematician Edward Waring said that the following theorem would probably be very difficult to prove because there was no adequate notation for primes. Gauss then proved it (while standing on one foot, it is rumored); he suggested that Waring failed for lack of notions, not notations.

**Theorem** (Wilson's Theorem). *If  $p$  is a prime, then*

$$(p - 1)! \equiv -1 \pmod{p}$$


Prove Wilson's Theorem. *Hint:* While standing on one foot, think about pairing each term in  $(p - 1)!$  with its multiplicative inverse.

### Problem 3.

Suppose  $a, b$  are relatively prime integers greater than 1. In this problem you will prove that Euler's function is *multiplicative*, that is, that

$$\phi(ab) = \phi(a)\phi(b).$$

The proof is an easy consequence of the Chinese Remainder Theorem.<sup>1</sup>

 2015, Albert R Meyer. This work is available under the terms of the [Creative Commons Attribution-ShareAlike 3.0 license](https://creativecommons.org/licenses/by-sa/3.0/).

<sup>1</sup>The *Chinese Remainder Theorem* asserts that if  $a, b$  are relatively prime and greater than 1, then for all  $m, n$ , there is a *unique*  $x \in [0..ab)$  such that

$$\begin{aligned} x &\equiv m \pmod{a}, \\ x &\equiv n \pmod{b}. \end{aligned}$$

A proof appears in Problem 8.55.

(a) Conclude from the Chinese Remainder Theorem that the function  $f : [0..ab) \rightarrow [0..a) \times [0..b)$  defined by

$$f(x) ::= (\text{rem}(x, a), \text{rem}(x, b))$$

is a bijection.

(b) For any positive integer,  $k$ , let  $\mathbb{Z}_k^*$  be the integers in  $[0..k)$  that are relatively prime to  $k$ . Prove that the function  $f$  from part (a) also defines a bijection from  $\mathbb{Z}_{ab}^*$  to  $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$ .

(c) Conclude from the preceding parts of this problem that

$$\phi(ab) = \phi(a)\phi(b). \tag{1}$$

(d) Prove Corollary 8.10.11: for any number  $n > 1$ , if  $p_1, p_2, \dots, p_j$  are the (distinct) prime factors of  $n$ , then

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_j}\right).$$