

# CS 135

## Modular structures, 2

Professor Bloom

March 17, 2009

### 1 $\mathbb{Z}_m^*$

Remember that for  $m \geq 1$ ,  $\mathbb{Z}_m^*$  is the set of numbers  $x$  in the range  $1 \leq x < m$  which are relatively prime to  $m$ .

Euler introduced the “phi function”  $\varphi(m)$  which is the size of  $\mathbb{Z}_m^*$ . This function has many nice properties.

**Proposition 1.1** 1. If  $p$  is prime,  $\varphi(p) = p - 1$ .

2. If  $p$  is prime and  $n \geq 1$ , then  $\varphi(p^n) = p^n - p^{n-1}$ .

3. If  $m, n$  are relatively prime, then  $\varphi(mn) = \varphi(m)\varphi(n)$ .

*Proof.*

1. When  $p$  is prime, every number  $x$  in the range  $1 \leq x < p$  is relatively prime to  $p$ .
2. When  $p$  is prime, which numbers  $x$  in the range  $1 \leq x < p^n$  are NOT relatively prime to  $p^n$ ? Those numbers which are divisible by  $p$ . What are they?

$$p, 2p, 3p, \dots, (p^{n-1} - 1)p,$$

so that there are  $p^{n-1} - 1$  numbers that are not relatively prime to  $p^n$ . Hence

$$\begin{aligned}\varphi(p^n) &= (p^n - 1) - (p^{n-1} - 1) \\ &= p^n - p^{n-1}.\end{aligned}$$

3. We postpone the proof of the last claim until we have some more facts.

**Proposition 1.2** *Suppose  $m, n$  are relatively prime. If  $x$  is an integer such that  $m|x$  and  $n|x$ , then  $(mn)|x$ .*

*Proof.* Since  $\gcd(m, n) = 1$ , there are integers  $a, b$  such that

$$an + bm = 1.$$

Now  $x = qn = q'm$ , for some integers  $q, q'$ . Thus,

$$\begin{aligned} x &= anx + bmx \\ &= anq'm + bmqn \\ &= (aq' + bq)mn, \end{aligned}$$

showing that  $(mn)|x$ .

**Proposition 1.3** *Suppose that  $m, n$  are relatively prime,  $1 \leq u < mn$  and  $\gcd(u, mn) = 1$ . Then if  $x = (u \bmod m)$ , then  $\gcd(x, m) = 1$ . Similarly, if  $y = (u \bmod n)$ , then  $\gcd(y, n) = 1$ .*

*Proof.* We start with the fact that

$$au + bmn = 1, \tag{1}$$

for some integers  $a, b$ . Now we show that there are integers  $\alpha, \beta$  such that

$$\alpha x + \beta m = 1.$$

Since  $x = (u \bmod m)$ ,

$$u - x = qm,$$

for some  $q$ . Thus,  $u = qm - x$ . Replacing  $u$  by  $qm - x$  in (1), we have

$$a(qm - x) + bmn = 1.$$

But

$$a(qm - x) + bmn = (-a)x + Qm,$$

for  $Q = (aq + bn)$ . Thus, let  $\alpha = -a$  and  $\beta = (aq + bn)$ . A similar argument shows that  $u \bmod n$  is relatively prime to  $n$ .

We consider the converse.

**Proposition 1.4** *If  $0 < u$  then  $u \perp mn$  if and only if  $(u \bmod n) \perp n$  and  $(u \bmod m) \perp m$ .*

*Proof.* We have just proved one way in the previous Proposition: if  $u \perp mn$  then  $u \perp n$  and  $u \perp m$ .

Conversely, remember  $u \perp n$  iff  $(u \bmod n) \perp n$ , since if  $1 = xu + yn$ , and  $u = qn + (u \bmod n)$ , then

$$\begin{aligned} 1 &= x(qn + (u \bmod n)) + yn \\ &= x(u \bmod n) + (xq + y)n. \end{aligned}$$

If it is not the case that  $u \perp mn$ , then some prime  $p$  divides both  $u$  and  $mn$ . But since  $m \perp n$ ,  $p$  either divides both  $u$  and  $n$  or both  $u$  and  $m$ . But this contradicts the fact that  $u$  is relatively prime to both  $n$  and  $m$ .

**Theorem 1.5** *The function  $\mathbb{Z}_{mn}^* \rightarrow \mathbb{Z}_n^* \times \mathbb{Z}_m^*$  taking  $u \in \mathbb{Z}_{mn}^*$  to*

$$(u \bmod n, u \bmod m)$$

*is a bijection.*

The fact that if  $u \perp mn$  then  $(u \bmod n, u \bmod m)$  is in  $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$ , follows from the previous proposition 1.3. The map is injective, since if  $u \equiv v \pmod{n}$  and  $u \equiv v \pmod{m}$ , then  $mn|u-v$ , by Prop. 1.2. Thus, if both  $u, v < mn$ ,  $u = v$ .

Why is the map onto?

**Chinese Remainder Theorem.** Suppose that  $m \perp n$ , and  $a, b$  are any integers. Then, there is a unique integer  $0 \leq u < mn$  such that

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

Any other solution has the form  $u + qmn$ , for some integer  $q$ .

*Proof.* Since  $n \perp m$ , there are integers  $x, y$  such that

$$1 = xn + ym.$$

But then

$$\begin{aligned} xn &\equiv \begin{cases} 1 & \pmod{m} \\ 0 & \pmod{n}. \end{cases} \\ ym &\equiv \begin{cases} 0 & \pmod{m} \\ 1 & \pmod{n}. \end{cases} \end{aligned}$$

Thus,

$$b(xn) + a(y m) \equiv \begin{cases} a & \pmod{n} \\ b & \pmod{m} \end{cases}$$

Then, let  $u = (axn + bym) \bmod mn$ . Then  $u < mn$  and  $u \bmod n \equiv a$  and  $u \bmod m = b$ .

If  $z$  is any solution, then  $z \equiv u \pmod{n}$  and  $z \equiv u \pmod{m}$ , so that  $z \equiv u \pmod{nm}$ , proving the last claim.  $\square$

So we ask again: why is the map  $\mathbb{Z}_{mn}^* \rightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*$  onto?

Let  $a \in \mathbb{Z}_m^*$ ,  $b \in \mathbb{Z}_n^*$ . Then, by the Chinese remainder theorem, there is some  $0 < u < mn$  such that

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

Thus,  $(u \bmod m) = a$  and  $(u \bmod n) = b$ . Since  $a \perp m$  and  $b \perp n$ , we know  $u \perp mn$ . This shows the map is onto, completing the proof of the theorem.

**Corollary 1.6** *If  $n \perp m$ , then  $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ .*  $\square$

This is just a restatement of Theorem 1.5.

## 2 Exercises

1. Read Section 3.7 in Rosen
2. Show: if  $u, v \in \mathbb{Z}_n^*$ , then  $(uv) \bmod n \in \mathbb{Z}_n^*$ ; i.e.,  $\mathbb{Z}_n^*$  is closed under multiplication mod  $n$ .
3. Show: if  $u \in \mathbb{Z}_n^*$ , then there is some  $v \in \mathbb{Z}_n^*$  such that  $(uv) \bmod n = 1$ ; so each element in  $\mathbb{Z}_n^*$  has a multiplicative inverse.
4. Generalize the Chinese remainder theorem to the case that there are  $k \geq 2$  integers,  $m_1, \dots, m_k$ , relatively prime in pairs. Show that there is a solution  $x$  to the set of equations

$$x \equiv a_i \pmod{m_i},$$

$i = 1, 2, \dots, k$ , for any integers  $a_1, \dots, a_k$ .

5. Show that if  $m_1, \dots, m_k$  are any  $k$  integers, then the greatest common divisor  $d$  of this set can be written as

$$d = x_1 m_1 + \dots + x_k m_k,$$

for some integers  $x_1, \dots, x_k$ . *Hint:* Let  $X$  be the set of all numbers of the form  $x_1 m_1 + \dots + x_k m_k$ . Show:

- $u, v \in X \implies u + v \in X$  and  $u - v \in X$ .

- $u \in X$  implies  $au \in X$ , for any integer  $a$ .
- Each of  $m_1, \dots, m_k \in X$ .
- There is some positive number in  $X$
- Suppose  $d$  is the *smallest* positive number in  $X$ .
- Show that if  $u \in X$ , then  $d|u$ . (Write  $u = qd + r$ , where  $0 \leq r < d$ . Since  $u, d \in X$ , then  $r = u - qd \in X$ .)