

1 Lists of exponents

Take any a, b in \mathbb{Z}_n^* (remember this means that a and b are coprime to n). Consider the set:

$$S_a = \{1, a, a^2, a^3 \dots\}$$

(This is just the set containing all powers of a modulo n that we saw in lecture.)

Now, let's create a second set by multiplying the first set by b :

$$S_b = \{b, ba, ba^2, ba^3, \dots\}$$

1.1 Case 1 (20 points)

If $b \in S_a$ then $b = a^k$ for some k , and $S_b = \{a^k, a^{k+1}, a^{k+2}, \dots\}$. But since a is coprime to n , the powers of a must cycle back to 1 every $\phi(n)$ steps. In particular, S_b will contain 1, and every power of a after that, which by definition is the set S_a . Furthermore, since every element of S_b is a power of a , it is contained in S_a as well, so the two sets are equal.

1.2 Case 2 (20 points)

Suppose for contradiction that there exists an element in both S_a and S_b . Let $x = ba^k$ be the first such element in S_b , that is, the one with the smallest exponent k (by assumption, we must have $k > 0$). Then $ba^k = a^j$ for some $j \geq 0$. But then $ba^{k-1} = a^{j+\phi(n)-1}$ (since $a^{\phi(n)} = 1$, since a and n are coprime). Thus, ba^{k-1} is also in S_a , contradicting the choice of k as the smallest exponent. We have a contradiction, and conclude that there is no such element.

1.3 Common factors (10 points)

If a is not coprime to n , it need never cycle back to 1 (e.g. powers of 2 mod 10), so the first time through the powers of a will be different than the later ones. This means that if b starts as a higher power of a , it may never loop back all the way to cover the beginning of the list.

2 Extended Euclid (25 points)

$$419 = 6883 \bmod 808 = 6883 - 8(808)$$

$$389 = 808 \bmod 419 = 808 - 419 = 808 - [6883 - 8(808)] = -6883 + 9(808)$$

$$30 = 419 \bmod 389 = 419 - 389 = [6883 - 8(808)] - [-6883 + 9(808)] = 2(6883) - 17(808)$$

$$29 = 389 \bmod 30 = 389 - 12(30) = [-6883 + 9(808)] - 12[2(6883) - 17(808)] = -25(6883) + 213(808)$$

$$1 = 30 \bmod 29 = 30 - 29 = [2(6883) - 17(808)] - [-25(6883) + 213(808)] = 27(6883) - 230(808)$$

3 Broken Chinese Remainder (25 points)

$84 = 0 \bmod 12$ and 14 , making it a duplicate of 0 .

(More generally: $a + 84 = a$ modulo both 12 and 14 .)

4 Fixed Chinese Remainder (20 points extra credit)

Given the value $a \bmod 14$, since 7 is a factor of 14 we can take its value modulo 7 to get the value of $a \bmod 7$. Thus, given CRR modulo 12 and 14 we can determine the values mod 12 and 7 . By the Chinese Remainder Theorem, since 12 and 7 are coprime, these moduli uniquely determine the value of a modulo $12 \cdot 7 = 84$.