Reviewing a few results in Number Theory

Aditya Ghosh

1. In modular arithmetic, a residue of an integer a in modulo n is the unique value of $0 \leq r \leq n-1$ such that $a = kn + r$. In the context of division, a residue is simply a remainder. A *residue class* is a complete set of integers that are congruent modulo n for some positive integer n. In modulo n, there are exactly n different residue classes, corresponding to the n possible residues $\{0, 1, 2, 3, \ldots, n-2, n-1\}$.

   Each residue class contains all integers in the form $kn + r$ where r is the corresponding residue. Note that $\{kn + r : k \geq 0\}$ is an arithmetic progression.

2. A *complete residue system* modulo n is a set of integers which satisfy the following condition: Every integer is congruent to a unique member of the set modulo n.

   In other words, the set contains exactly one member of each residue class.

   Examples: $\{1, 2, 3\}$, $\{4, 5, 6\}$, and $\{9, 17, 85\}$ are all Complete residue systems $(\mathrm{mod}\ 3)$. $\{k, k+1, k+2, k+3, \ldots, k+m-1\}$ is a complete residue system $(\mathrm{mod}\ m)$, for any integer k and positive integer m. Basically, any consecutive string of m integers forms a complete residue system $(\mathrm{mod}\ m)$.

3. A subset R of the integers is called a *reduced residue system* modulo n if every integer coprime to n is congruent to a unique member of the set R.

   We can easily see that, R is a reduced residue system modulo n if: (i) $\gcd(r, n) = 1$ for each r in R, (ii) R contains $\phi(n)$ elements, and (iii) no two elements of R are congruent modulo n.

   A reduced residue system modulo n can be formed from a complete residue system modulo n by removing all integers not relatively prime to n. For example, a complete residue system modulo 12 is $\{0, 1, 2, 3, \ldots, 10, 11\}$. Observe that $1, 5, 7$ and 11 are the only integers in this set which are relatively prime to 12, and so the corresponding reduced residue system modulo 12 is $\{1, 5, 7, 11\}$. Note that it has $\phi(12) = 4$ elements.

   Some other reduced residue systems modulo 12 are: $\{13, 17, 19, 23\}$, $\{-11, -7, -5, -1\}$, $\{-7, -13, 13, 31\}$ etc.

4. Fermat's theorem. Let p be a prime and a be an integer not divisible by p. Then, $a^{p-1} - 1$ is a multiple of p.

   Basic idea behind this is that $\{a, 2a, 3a, \ldots, (p-1)a\}$ is a complete residue system modulo p. So if we multiple these numbers modulo p, that will be same as multiplying $\{1, 2, \ldots, p-1\}$. Thus, $a \times 2a \times \cdots \times (p-1)a \equiv 1 \times 2 \times \cdots \times (p-1)$ (mod p), which implies $(p-1)!a^{p-1} \equiv (p-1)!$ (mod p) $\implies a^{p-1} \equiv 1$ (mod p).

5. Euler's theorem. Let n be a any positive integer and a be an integer coprime to n. Then $a^{\phi(n)} - 1$ is a multiple of n.

Instead of complete residue system, we consider a reduced residue system here. Suppose $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ is a reduced residue system modulo n. You can in fact show that $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ is also a reduced residue system modulo n iff a is coprime to n. Then, multiplying the elements of the last set modulo n is same as multiplying the elements of the former. Hence, $ar_1 \times ar_2 \times \cdots \times ar_{\phi(n)} \equiv r_1 \times r_2 \times \cdots \times r_{\phi(n)} \pmod{n}$, which yields $a^{\phi(n)} \equiv 1 \pmod{n}$.

6. Bezout's theorem. For any two integers a, b (not both zero), we can express their gcd as a linear combination of themselves, i.e. there exists integers x, y such that $\gcd(a, b) = ax + by$. The existence of such integers x, y follows from the Euclidean algorithm that we use to find $\gcd(a, b)$. Note, x, y need not be unique. In fact, if x_0, y_0 is a solution of the equation then $x = x_0 + bt, y = y_0 - at$ will also be a solution for any integer t.

7. Special case: when a, b are coprime, Bezout's theorem tells us that $ax + by = 1$ for some integers x, y. The converse is also true: if there exist integers x, y such that $ax + by = 1$, then you can show that a, b must be coprime. This gives us the idea of modular inverse.

8. Modular inverse. Suppose n is a positive integer. A number a' is said to be an inverse of a modulo n if $aa' = 1 \pmod{n}$. It is easy to show that a has an inverse modulo n iff a is coprime to n. Furthermore, the inverse a' is unique modulo n.

   Example: $2 \times 3 \equiv 1 \pmod{5}$, so 2 and 3 are inverses of each other modulo 5.

9. Wilson's theorem. Suppose p is a prime. Then, $(p-1)! \equiv -1 \pmod{p}$.

   Proof. The positive integers $\{1, 2, \ldots, p-1\}$ are coprime to p, so each of them has an inverse modulo p. Note that $a^2 \equiv 1 \pmod{p}$ iff $a = 1$ or $p - 1$. Therefore each of the numbers $\{2, 3, \ldots, p-2\}$ has an inverse different from themselves, and its not hard to see that no two of them will have the same inverse. Therefore, we can pair them up as $\{a, b\}$ such that $ab \equiv 1 \pmod{p}$. Multiplying the pairs, we get $(p-2)! \equiv 1 \pmod{p}$, which yields $(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$. □

   In fact, we can show that $n \mid (n-1)! + 1 \iff n$ is a prime.

10. Let p be an odd prime. Then, (i) $p \mid n^2 + 1$ for some n only if $p \equiv 1 \bmod 4$.
    (ii) If $p \equiv 1 \bmod 4$, then there exists some n such that $p \mid n^2 + 1$.

    Proof. (i) Use Fermat's theorem. (ii) Use Wilson's theorem.

11. Chinese Remainder theorem. Suppose we are seeking integer x satisfying $x = a \pmod{m}$ and $x = b \pmod{n}$. The theorem says that if m, n are coprime then there exists such x and it is in fact unique modulo mn.

    For a more general version of CRT, read David Burton's book or K.Conrad's note.