Number Theory

Trong

Sat Dec 1, 2018—December 2, 2018

Contents

1 Congruences

Theorem 1 (Divisor Sum)**.** *For any natural number n,*

$$\sum_{d|n} \varphi(d) = n,$$

where $\varphi(d)$ is the Euler Totient function.

Proof. Consider the set $A(d) = \{k : (k, n) = d\}$. For each k, define l s.t. $k = dl$. Then it's easy to see that $(l, \frac{n}{d}) = 1$. In fact, there is a one-to-one correspondence between k and l, so that $|A(d)| = |\{k\}| = |\{l\}|$. Now the l's are numbers less than $\frac{n}{d}$ and coprime with it, so $|A(d)| = \varphi(\frac{n}{d})$.

Next, note that the sets $A(d)$ for distinct $d|n$ are disjoint and their union is $1, \ldots, n$. Therefore

$$n = \sum_{d|n} |A(d)| = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

Finally

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d),$$

since the divisors $\frac{n}{d}$ in the first sum are the same as the divisors d in the second sum. □

Problem 2. *Find integers $a_1, \ldots, a_5$ s.t. every integer x*

satisfies at least one of the congruences

$$\begin{aligned}
x &\equiv a_1 \bmod 2 \\
x &\equiv a_2 \bmod 3 \\
x &\equiv a_3 \bmod 4 \\
x &\equiv a_4 \bmod 6 \\
x &\equiv a_5 \bmod 12. \qquad (*)
\end{aligned}$$

Solution. Consider the remainder classes mod 3:

$$\begin{aligned}
&3n \\
&3n+1 \\
&3n+2.
\end{aligned}$$

Substitute $2k$ and $2k+1$ for n, and take their remainders mod 2, 3, and 6:

$$\begin{aligned}
3 \cdot 2k &\equiv 0 \bmod 2 \\
3(2k+1) = 6k+3 &\equiv 0 \bmod 3 \\
3 \cdot 2k+1 = 6k+1 &\equiv 1 \bmod 6 \\
3(2k+1)+1 = 6k+4 &\equiv 0 \bmod 2 \\
3 \cdot 2k+2 &\equiv 0 \bmod 2 \\
3(2k+1)+2 = 6k+5 &\equiv 5 \bmod 6.
\end{aligned}$$

We've now covered every integer with mods 2, 3, and 6; if we can somehow write integers 5 mod 6 as either a_3 mod 4 or

$a_5 \bmod 12$, then we will have expressed every integer in the form $(*)$. Let's do that:

$$\begin{aligned} 6 \cdot 2k + 5 = 12k + 5 = 4(3k+1) + 1 &\equiv 1 \bmod 4 \\ 6(2k+1) + 5 = 12k + 11 &\equiv 11 \bmod 12. \end{aligned}$$

Therefore every integer x satisfies at least one of

$$\begin{aligned} x &\equiv 0 \bmod 2 \\ x &\equiv 0 \bmod 3 \\ x &\equiv 1 \bmod 4 \\ x &\equiv 1 \bmod 6 \\ x &\equiv 11 \bmod 12. \end{aligned}$$

□