BASIC PROPERTIES OF CONGRUENCES

The letters a, b, c, d, k represent integers. The letters m, n represent positive integers. The notation $a \equiv b \pmod{m}$ means that m divides $a - b$. We then say that a is congruent to b modulo m.

1. (Reflexive Property): $a \equiv a \pmod{m}$

2. (Symmetric Property): If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

3. (Transitive Property): If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Remark: The above three properties imply that "$\equiv \pmod{m}$" is an equivalence relation on the set $\mathbf{Z}$.

4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $a - c \equiv b - d \pmod{m}$.

5. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

6. Assume that $a \equiv b \pmod{m}$. Let $k \geq 1$. Then $a^k \equiv b^k \pmod{m}$.

7. Suppose that $P(x)$ is any polynomial with coefficients in $\mathbf{Z}$. Assume that $a \equiv b \pmod{m}$. Then $P(a) \equiv P(b) \pmod{m}$.

8. Assume that $a \equiv b \pmod{m}$. Then $gcd(a, m) \ = \ gcd(b, m)$.

9. If $a \equiv b \pmod{m}$ and $n \mid m$, then $a \equiv b \pmod{n}$.

10. Assume that $gcd(m, n) = 1$. Assume that $a \equiv b \pmod{m}$ and that $a \equiv b \pmod{n}$. Then $a \equiv b \pmod{mn}$.

11. Suppose that $a \in \mathbf{Z}$. Then there exists a unique integer r such that $a \equiv r \pmod{m}$ and $0 \leq r \leq m - 1$. This integer r is the remainder when a is divided by m.

12. Assume that $ca \equiv cb \pmod{m}$ and that $(c, m) = 1$. Then $a \equiv b \pmod{m}$.

13. Assume p is a prime. If $ab \equiv 0 \pmod{p}$, then either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

14. Assume that p is a prime and that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.