Geoffrey Parker - grp352
HW 2: 1.15 - 1.20, A.10, A.18
M328K
January 24th, 2012

1.15 Exercise. *Let a, b, and n be integers with $n > 0$. Show that if $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.*

Proof. Let a, b, and n be integers with $n > 0$ and $a \equiv b \pmod{n}$. We will show that $a^2 \equiv b^2 \pmod{n}$. First, since $a \equiv b \pmod{n}$, by definition of congruence mod n, $n \mid (a-b)$. Then, by Theorem 1.8, we can show that $n \mid (a-b)(a+b)$, since $(a+b)$ is an integer. So $n \mid (a^2-b^2)$. Therefore, by the definition of congruence mod n, $a^2 \equiv b^2 \pmod{n}$. □

1.16 Exercise. *Let a, b, and n be integers with $n > 0$. Show that if $a \equiv b \pmod{n}$, then $a^3 \equiv b^3 \pmod{n}$.*

Proof. Let a, b, and n be integers with $n > 0$ and $a \equiv b \pmod{n}$. We will show that $a^3 \equiv b^3 \pmod{n}$. First, since $a \equiv b \pmod{n}$, by definition of congruence mod n, $n \mid (a-b)$. Then, by Theorem 1.8, we can show that $n \mid (a-b)(a^2+ab+b^2)$, since (a^2+ab+b^2) is an integer. So $n \mid (a^3-b^3)$. Therefore, by the definition of congruence mod n, $a^3 \equiv b^3 \pmod{n}$. □

1.17 Exercise. *Let a, b, k, and n be integers with $n > 0$ and $k > 1$. Show that if $a \equiv b \pmod{n}$ and $a^{k-1} \equiv b^{k-1} \pmod{n}$, then*

$$a^k \equiv b^k \pmod{n}.$$

Proof. Let a, b, k, and n be integers with $n > 0$ and $k > 1$. Also, $a \equiv b \pmod{n}$ and $a^{k-1} \equiv b^{k-1} \pmod{n}$. We will show that $a^k \equiv b^k \pmod{n}$. Since $a^{k-1} \equiv b^{k-1} \pmod{n}$, $n \mid (a^{k-1}-b^{k-1})$, by the definition of congruence mod p. Then, by theorem 1.8, $n \mid (a^{k-1}-b^{k-1}) \times \frac{(ab(a^k-b^k))}{(ba^k-ab^k)}$. So $n|(a^k-b^k)$ which, by the definition of congruence mod n, means that $a^k \equiv b^k \pmod{n}$. □

1.18 Theorem. *Let a, b, k, and n be integers with $n > 0$ and $k > 0$. If $a \equiv b \pmod{n}$, then*

$$a^k \equiv b^k \pmod{n}.$$

Proof. Let a, b, k, and n be integers with $n > 0$ and $k > 0$ and $a \equiv b \pmod{n}$. We will show that $a^k \equiv b^k \pmod{n}$. First, by theorem 1.15, we know that $a^2 \equiv b^2 \pmod{n}$. Since theorem 1.17 demonstrates that for any integer $j \geq 1$, $a^j \equiv b^j \pmod{n}$ implies that $a^{j+1} \equiv b^{j+1} \pmod{n}$. So we have proved by induction that $a^k \equiv b^k \pmod{n}$. □

1.19 Exercise. *Illustrate each of Theorems* 1.12-1.18 *with an example using actual numbers.*

1. Example for 1.12: $9 \equiv 5 \pmod{4}$ and $7 \equiv 3 \pmod{4}$. So, $(9 + 7) - (5 + 3) = 16 - 8 = 8$ and $4 \mid 8$.

2. Example for 1.13: $12 \equiv 3 \pmod{3}$ and $17 \equiv 8 \pmod{3}$. So, $(12-17)-(3-8) = (-5) - (-5) = 0$ and $3 \mid 0$.

3. Example for 1.14: $6 \equiv 4 \pmod{2}$ and $7 \equiv 3 \pmod{2}$. So, $6 \times 7 - 4 \times 3 = 42 - 12 = 30$ and $2 \mid 30$.

4. Example for 1.15: $17 \equiv 12 \pmod{5}$. So $17^2 - 12^2 = 289 - 144 = 145$ and $5 \mid 145$.

5. Example for 1.16: $13 \equiv 4 \pmod{3}$. So $13^2 - 4^2 = 169 - 16 = 153$ and $3 \mid 153$.

6. Example for 1.17: $19 \equiv 7 \pmod{6}$ and $19^4 \equiv 7^4 \pmod{6}$ (that is $130321 \equiv 2401 \pmod{6}$. $130321 - 2401 = 127920 = 21320 \times 6$.) $19^5 - 7^5 = 2476099 - 16807 = 2459292 = 409882 * 6$

7. Example for 1.18: $7 \equiv 2 \pmod{5}$. So $7^6 - 2^6 = 117649 - 64 = 117585 = 23517$

1.20 Question. *Let a, b, c, and n be integers for which $ac \equiv bc \pmod{n}$. Can we conclude that $a \equiv b \pmod{n}$? If you answer "yes", try and give a proof. If you answer "no", try and give a counterexample.*

Solution. No. $10 \equiv 15 \pmod{5}$, so $2 \times 5 \equiv 3 \times 5 \pmod{5}$, yet $2 \not\equiv 3 \pmod{5}$. □

A.10 Theorem. *Let n be a natural number. Then* $1+2+3+\cdots+n = \frac{(n)(n+1)}{2}$

Proof. Proof by induction.

- Base Case $(n=1)$: $\frac{1(1+1)}{2} = 1$. True.
- Induction Hypothesis: There exists some natural number N such that $1+2+3+\cdots+N = \frac{(N)(N+1)}{2}$
- Then, $\frac{(N+1)(N+2)}{2} = \frac{(N)(N+1)+2(N+1)}{2} = \frac{(N)(N+1)}{2} + (N+1)$
  So by the induction hypothesis, this equals $1+2+3+\cdots+N+(N+1)$
  Therefore $\frac{(N)(N+1)+2(N+1)}{2} = 1+2+3+\cdots+(N+1)$.

□

A.18 Theorem. *For every natural number n,* $1+2+2^2+\cdots+2^n = 2^{n+1}-1$

Proof. Proof by induction:

- Base Case $(n=1)$: $1+2^1 = 3$ and $2^{1+1}-1 = 4-1 = 3$. True.
- Induction Hypothesis: There exists some natural number N such that $1+2+2^2+\cdots+2^N = 2^{N+1}-1$.
- So, $2^{(N+1)+1}-1 = 2(2^{N+1})-1 = 2(2^{N+1}-1)+1$. By the induction hypothesis, this equals $(1+2+2^2+\cdots+2^N)2+1 = (2+2^2+2^3+\cdots+2^{N+1})+1$. Therefore, $2^{(N+1)+1}-1 = 1+2+2^2+\cdots+2^{N+1}$.

□