Number Theory ☎

Jonas Wechsler

January 2015

Theorem 0.1.

$$\left.\begin{array}{l} a,b,c \in \mathbb{Z} \\ a|b \\ a|c \end{array}\right\}$$

$\implies a|(b+c)$

Proof. $a|b \implies \exists k \in \mathbb{Z} \ni ak = b$
$a|c \implies \exists j \in \mathbb{Z} \ni aj = c$
$b + c = ak + aj$ by substitution
$b + c = a(k + j)$ by factoring
$k, j \in \mathbb{Z} \implies k + j \in \mathbb{Z}$
$a|(b + c)$ by definition "|". ■

□

Theorem 0.2. *Theorem:*

$$\left.\begin{array}{l} a,b,c \in \mathbb{Z} \\ a|b \\ a|c \end{array}\right\}$$

$\implies a|(b-c)$
Proof: $a|b \implies \exists k \in \mathbb{Z} \ni ak = b$
$a|c \implies \exists j \in \mathbb{Z} \ni aj = c$
$b - c = ak - aj$ *by substitution*
$b - c = a(k - j)$ *by factoring*
$k, j \in \mathbb{Z} \implies k + j \in \mathbb{Z}$
$a|(b + c)$ *by definition "|".* ■

Theorem 0.3. *Theorem:*

$$\left.\begin{array}{l} a,b,cin\mathbb{Z} \\ a|b \\ a|c \end{array}\right\}$$

Proof: $a|b \implies \exists k \in \mathbb{Z} \ni ak = b$
$a|c \implies \exists j \in \mathbb{Z} \ni aj = c$
$akc = bc$ *by algebra*
Let $l \in \mathbb{Z} \ni l = kc$
$al = bc$ *by substitution*
$a|bc$ *by definition*

Theorem 0.4. 1.3 *can be reduced to* If $a|b$, then $a|bc$. 1.3 *can also be reworked to* If $a|b$ and $a|c$, then $a^2|bc$.

1. $a|b$
   $an = b$ *by definition*
   $anc = bc$ *by algebra*
   $\exists m \in \mathbb{Z} \ni am = bc$ *and* $m = nc$
   $a|bc$ *by definition*

2. $a|b$ *and* $a|c$
   $an = b$ *by def*
   $am = c$ *by def*
   $anam = bc$ *by algebra*
   $a^2nm = bc$ *by algebra*
   $a^2|bc$ *by definition*

Theorem 0.5. *Let* $a, b, c \in \mathbb{Z}$. *If* $a|b$, *then* $a|b^n$.
$a|b$
$an = b$ *by def*
$anb = bb$ *by algebra*
$\exists m \in \mathbb{Z} \ni am = bb$ *and* $m = nb$
$am = b^2$ *by algebra*

Theorem 0.6. $a|b$
$an = b$ *by definition*
$anc = bc$ *by algebra*
$\exists m \in \mathbb{Z} \ni am = bc$ *and* $m = nc$
$a|bc$ *by definition*

Theorem 0.7. *1* $45 \equiv 9 \pmod 4$*?*
$\exists m \in \mathbb{Z}|m(4) + 9 = 45$
$4m + 9 = 45$
$4m = 36$
$m = 9$
Yes

2 $37 \equiv 2 \pmod 5$*?*
$\exists m \in \mathbb{Z}|m(5) + 2 = 37$
$5m + 2 = 37$
$5m = 35$
$m = 7$
Yes

3 $37 \equiv 3 \pmod 5$*?*
$\exists m \in \mathbb{Z}|m(5) + 3 = 37$
$5m + 3 = 37$
$5m = 34$
No

4 $37 \equiv -3 \pmod 5$*?*
$\exists m \in \mathbb{Z}|m(5) - 3 = 37$
$5m - 3 = 37$
$5m = 40$
$m = 8$
Yes

Theorem 0.8. *1* $m \equiv 0 \pmod 3$
$\exists n \in \mathbb{Z} | n(3) + 0 = m$
$3n + 0 = m$

2 $m \equiv 1 \pmod 3$
$\exists n \in \mathbb{Z} | n(3) + 1 = m$
$3n + 1 = m$

3 $m \equiv 2 \pmod 3$
$\exists n \in \mathbb{Z} | n(3) + 2 = m$
$3n + 2 = m$

4 $m \equiv 3 \pmod 3$
$\exists n \in \mathbb{Z} | n(3) + 3 = m$
$3n + 3 = m$

5 $m \equiv 4 \pmod 3$
$\exists n \in \mathbb{Z} | n(3) + 4 = m$
$3n + 4 = m$

Theorem 0.9. *1* $n \equiv b \pmod k$
$k|(n-b)$ *def of mod*
$\exists ak = n - b$ *def of "|"*
$ak + b = n$

Theorem 0.10. *Theorem:*

$$\left.\begin{array}{l} a, n \in \mathbb{Z} \\ n \;>\; 0 \end{array}\right\}$$

$\implies a \equiv a \mod n$
Proof: $n0 = 0$ *by algebra*
$a - a = 0$ *by algebra*
$\exists k \in \mathbb{Z} \ni k = 0$
$nk = 0$ *by substitution*
$nk = a - a$ *by substitution*
$n|a - a$ *by definition*
$a \equiv a \mod n$ *by definition* ■

Theorem 0.11. *Theorem:*

$$\left.\begin{array}{l} a, b, n \in \mathbb{Z} \\ n > 0 \\ a \equiv b \mod n \end{array}\right\}$$

$\implies b \equiv a \mod n$
Proof: $a \equiv b \mod n$
$n|(a-b)$ *by definition*
$\exists k \in \mathbb{Z} \ni nk = a - b$
$-nk = -a + b$ *by algebra*
$-kn = b - a$ *by algebra*
$n|(b-a)$ *by definition*
$b \equiv a \mod n$ *by definition* ■

Theorem 0.12. *Theorem:*

$$\left.\begin{array}{l} a,b,c,n \in \mathbb{Z} \\ n > 0 \\ a \equiv b \mod n \\ b \equiv c \mod n \end{array}\right\}$$

$\implies a \equiv c \mod n$
Proof: $a \equiv b \mod n$ *by definition*
$b \equiv c \mod n$ *by definition*
$n|(a-b)$ *by definition*
$n|(b-c)$ *by definition*
$nk = b - c \wedge nj = a - b$
$nk - nj = (b-c) + (a-b)$ *by algebra*
$n(k-j) = b - c + a - b$ *by algebra*
$n(k-j) = a - c$ *by algebra* $n|(a-c)$ *by definition*
$a \equiv c \mod n$ *by definition* ■

Theorem 0.13. *Theorem:*

$$\left.\begin{array}{l} a,b,c,d,n \in \mathbb{Z} \\ n > 0 \\ a \equiv b \mod n \\ c \equiv d \mod n \end{array}\right\}.$$

$\implies a + c \equiv b + d \mod n$
Proof:$a \equiv b \mod n$
$c \equiv d \mod n$
$n|(a-b)$ *by definition*
$n|(c-d)$ *by definition*
$n|(a-b) + (c-d)$ *by Thm 1.1*
$n|(a+c-b-d)$ *by algebra*
$n|((a+c)-(b+d))$ *by Algebra*
$a + c \equiv b + d \mod n$ *by definition* ■

Theorem 0.14. *Theorem:*

$$\left.\begin{array}{l} a,b,c,d,n \in \mathbb{Z} \\ n > 0 \\ a \equiv b \mod n \\ c \equiv d \mod n \end{array}\right\}$$

$\implies a - c \equiv b - d \mod n$
Proof:$a \equiv b \mod n$
$c \equiv d \mod n$
$n|(a-b)$ *by definition*
$n|(c-d)$ *by definition*
$n|((a-b)-(c-d))$ *by Thm 1.2*
$n|((a-c)-(b-d))$ *by Algebra*
$a - c \equiv b - d \mod n$ *by definition* ■

Theorem 0.15. *Theorem:*

$$\left.\begin{array}{l} a,b,c,d,n \in \mathbb{Z} \\ n > 0 \\ a \equiv b \mod n \\ c \equiv d \mod n \end{array}\right\}$$

$\implies ac \equiv bd \mod n$
Proof:$a \equiv b \mod n$

$c \equiv d \mod n$
$n|(a-b)$ *by definition*
$n|(c-d)$ *by definition*
$n|a$ *and* $n|b$ *and* $n|c$ *and* $n|d$
$n|ac$ *by Thm 1.3*
$n|ad$ *by Thm 1.3*
$n|((ac)-(bd)$ *by Thm 1.2*
$ac \equiv bd \mod n$ *by definition* ■

Theorem 0.16. *Theorem:*

$$\left.\begin{array}{l} a,b,n \in \mathbb{Z} \\ n > 0 \\ a \equiv b \mod n \end{array}\right\}$$

$\implies a^2 \equiv b^2 \mod n$
Proof: $a \equiv b \mod n$
$n|(a-b)$ *by defintion*
$n|a$ *and* $n|b$ *by definition*
$n|a^2$ *and* $n|b^2$ *by Thm 1.6*
$n|(a^2-b^2)$ *by Thm 1.2*
$a^2 \equiv b^2 \mod n$ *by defnition* ■

Theorem 0.17. *Theorem:*

$$\left.\begin{array}{l} a,b,n \in \mathbb{Z} \\ n > 0 \\ a \equiv b \mod n \end{array}\right\}$$

$\implies a^3 \equiv b^3 \mod n$
Proof: $a \equiv b \mod n$
$n|(a-b)$ *by defintion*
$n|a$ *and* $n|b$ *by definition*
$n|a^2$ *and* $n|b^2$ *by Thm 1.6*
$n|a^3$ *and* $n|b^3$ *by Thm 1.6*
$n|(a^3-b^3)$ *by Thm 1.2*
$a^3 \equiv b^3 \mod n$ *by defnition* ■

Theorem 0.18. *Theorem:*

$$\left.\begin{array}{l} a,b,k,n \in \mathbb{Z} \\ n > 0 \\ k > 1 \\ a \equiv b \mod n \\ a^{k-1} \equiv b^{k-1} \mod n \end{array}\right\}$$

$\implies a^k \equiv b^k \mod n$
Proof: $a \equiv b \mod n$
$a^{k-1} \equiv b^{k-1} \mod n$
$n|a$ *and* $n|b$ *and* $n|a^{k-1}$ *and* $n|b^{k-1}$ *by definition*
$n|(a^{k-1}a)$ *and* $n|(a^{k-1}a)$ *by Thm 1.3*
$n|a^k$ *and* $n|b^k$ *by algebra*
$n|(a^k-b^k)$ *by Thm 1.2*
$a^k \equiv b^k \mod n$ *by defintion*

Theorem 0.19. *Theorem:*

$$\left.\begin{array}{l} a,b,k,n \in \mathbb{Z} \\ n > 0 \\ k > 0 \\ a \equiv b \mod n \end{array}\right\}$$

$\implies a^k \equiv b^k \mod n$
Proof: $a \equiv b \mod n$
$n|a$ *and* $n|b$
$n|(a^k)$ *and* $n|(a^k)$ *by Thm 1.6*
$n|(a^k - b^k)$ *by Thm 1.2*
$a^k \equiv b^k \mod n$ *by defintion*

Theorem 0.20. $a \equiv b \mod c \implies c|(a-b) \implies ck = a - b$

1. $12 \equiv 2 \mod 5 \implies 5k = 12 - 2$
   $20 \equiv 5 \mod 5 \implies 5k = 20 - 5$
   $32 \equiv 7 \mod 5 \implies 5k = 32 - 7$

2. $12 \equiv 2 \mod 5 \implies 5k = 12 - 2$
   $20 \equiv 5 \mod 5 \implies 5k = 20 - 5$
   $-8 \equiv -3 \mod 5 \implies 5k = -8 + 3$

3. $12 \equiv 2 \mod 5 \implies 5k = 12 - 2$
   $20 \equiv 5 \mod 5 \implies 5k = 20 - 5$
   $240 \equiv 10 \mod 5 \implies 5k = 240 - 10$

4. $12 \equiv 2 \mod 5 \implies 5k = 12 - 2$
   $144 \equiv 4 \mod 5 \implies 5k = 144 - 4$

5. $12 \equiv 2 \mod 5 \implies 5k = 12 - 2$
   $1728 \equiv 8 \mod 5 \implies 5k = 1728 - 8$

6. $9 \equiv 5 \mod 2 \implies 2k = 9 - 5$
   $9^{4-1} \equiv 5^{4-1} \mod 2 \implies 2k = 729 - 125$
   $9^4 \equiv 5^4 \mod 2 \implies 2k = 6561 - 625$

7. $12 \equiv 2 \mod 5 \implies 5k = 12 - 2$
   $12^k \equiv 2^k \mod 5 \implies 5k = 12^k - 2^k$

Theorem 0.21. *Theorem:*

$$\left.\begin{array}{l} a,b,c,n \in \mathbb{Z} \\ ac \equiv bc \mod n \end{array}\right\}$$

$\implies a \equiv b \mod n$
Proof: $ac \equiv bc \mod n$
$n|(ac - bc)$ *by definition*
$nk = ac - bc$ *by definition*
$n\frac{k}{c} = a - b$ *by algebra*
If $c|k$*, then we can conclude that* $\exists j \in \mathbb{Z} \ni j = \frac{k}{c}$
In this case, $nj = a - b$ *by substitution,* $n|(a-b)$ *by definition, and* $a \equiv b \mod n$ *by definition.*

Theorem 0.22. *Theorem:*

$$\left.\begin{array}{l} n, m, a_i \in \mathbb{N} \\ 0 \leq a_i \leq 9 \\ n = a_k a_{k-1} ... a_1 a_0 \\ m = a_k + a_{k-1} ... + a_1 + a_0 \end{array}\right\}$$

$$\implies n \equiv m \mod 3$$

Proof. $n - m = (a_0\ 3|(n-m)$
$3k = n - m$

$\square$

Theorem 0.23.

Theorem 0.24.