CS 2050 Worksheet 6

4.1 Divisibility and Modular Arithmetic

1. Let a, b, c be integers, where $a \neq 0$. Prove that "if $a|b$ and $a|c$, then $a|(b+c)$."

p: a|b and a|c

q: a|(b+c)

1) a|b and a|c — assume p
2) $b = ak$, $k \in \mathbb{Z}$ — def'n of divisib.
3) $c = ak'$, $k' \in \mathbb{Z}$ — def'n of divisib.
4) $b+c = ak + ak'$ — add b+c
5) $b+c = a(k+k')$ — factor a
6) $k'' = k+k'$, $k'' \in \mathbb{Z}$ — def'n new variable
7) $b+c = ak''$ — sub k''
8) a|(b+c) — def'n of divisib.

Note: this is q

Conc: Since assuming p leads to q, I have proven p→q by direct proof.

2. Calculate a **div** m and a **mod** m for each of the following:

a) $a = 16 \quad m = 4$

16 div 4 = 4

16 mod 4 = 0

b) $a = 3 \quad m = 9$

3 div 9 = 0

3 mod 9 = 3

c) $a = 17 \quad m = 3$

17 div 3 = 5

17 mod 3 = 2

$$\begin{array}{r} 5 \\ 3\overline{)17} \\ 15 \\ \hline 2 \end{array}$$

17

d) $a = -17 \quad m = 3$

−17 div 3 = −6

−17 mod 3 = 1

−6(3) + 1

R must be greater than or equal to zero.

a (mod 13) = 4 (mod 13)

a = 4   b = 11

3. Let a and b be integers such that $a \equiv 4 \pmod{13}$ and $b \equiv 11 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ that satisfies each of the following:

b = −2 also

a) $c \equiv 7a \pmod{13}$

c (mod 13) = 7(4) (mod 13)

c (mod 13) = 28 (mod 13)

c (mod 13) = 2 (mod 13)

$\boxed{c = 2}$

$$\begin{array}{r} 28 \\ -13 \\ \hline 15 \\ -13 \\ \hline 2 \end{array}$$

16

14

b) $c \equiv a - b \pmod{13}$

c (mod 13) = (4 − 11) (mod 13)

c (mod 13) = −7 (mod 13)

c (mod 13) = 6 (mod 13)

$\boxed{c = 6}$

280

$$\begin{array}{r} 20 \\ 13 \\ \hline 60 \\ 200 \\ \hline 260 \end{array} \qquad \begin{array}{r} 22 \\ 13 \\ \hline 66 \\ 220 \\ \hline 286 \end{array}$$

c) $c \equiv 3a^2 + 2b^2 \pmod{13}$

a = 4   b = −2

c (mod 13) = $3(4)^2 + 2(-2)^2$ (mod 13)

$c \pmod{13} = 56 \pmod{13}$

$c \pmod{13} = 4 \pmod{13}$

$\boxed{c = 4}$

$56 + 13(-4)$

$56 + (-52) = 4$

4. Show that if $a \equiv b \pmod m$ and $c \equiv d \pmod m$, where a, b, c, d, and m are integers, then $ac \equiv bd \pmod m$.

p: $a \equiv b \pmod m$ and $c \equiv d \pmod m$

q: $ac \equiv bd \pmod m$

$ac = bd + Km$

1) $a \equiv b \pmod m$ and $c \equiv d \pmod m$ — assume p
2) $a = b + km,\ k \in \mathbb{Z}$ — def'n of mod equiv./congruence
3) $c = d + k'n,\ k' \in \mathbb{Z}$ — def'n of mod equiv./congruence
4) $a \cdot c = (b+km)(d+k'm)$ — multiply $a \cdot c$
5) $ac = bd + bk'm + dkm + kk'm^2$ — expand
6) $ac = bd + m(bk' + dk + kk'm)$ — factor m
7) $k'' = bk' + dk + kk'm,\ k'' \in \mathbb{Z}$ — define new variable
8) $ac = bd + k''m$ — sub k''
9) $ac \equiv bd \pmod m$ — def'n of mod equiv.

Note: this is q

Conc: since assuming p leads to q, I have proven $p \to q$ is true using direct proof.

5.1 Mathematical Induction

5. Use mathematical induction to prove that $1^3 + 2^3 + 3^3 + ... + n^3 = \frac{n^2(n+1)^2}{4}$ for $n \in \mathbb{Z}, n \geq 1$.

Base Step: I'll show $P(1)$ is true

$P(1)$: $1^3 = \frac{1^2(1+1)^2}{4}$ — LHS and RHS

$1 = \frac{1^2(1+1)^2}{4}$ — simplify LHS

$1 = \frac{1(1+1)^2}{4}$ — simplify

$1 = \frac{1(2)^2}{4}$ — simplify

$1 = \frac{1(4)}{4}$ — simplify

$1 = 1$ ✓ — cancel out 4 (simplify)

Conc: Therefore $P(1)$ is true, thus concluding the base case.

Inductive Step: I'll show $P(K) \to P(K+1)$

$\frac{(n+1)^2(n+2)^2}{4}$

$P(K)$: $1^3 + 2^3 + \dots + k^3 = \frac{k^2(k+1)^2}{4}$

$K \in \mathbb{Z}^+$

1) $P(K)$: $1^3 + 2^3 + \dots + k^3 = \frac{k^2(k+1)^2}{4}$ — assume $P(K)$
2) $1^3 + 2^3 + \dots + k^3 + (k+1)^3 = \frac{k^2(k+1)^2}{4} + (k+1)^3$ — add $(k+1)^3$ to each side
3) $= \frac{k^2(k+1)^2 + 4(k+1)^3}{4}$ — common denominator
4) $= \frac{(k+1)^2(k^2 + 4(k+1))}{4}$ — factor out $(k+1)^2$
5) $= \frac{(k+1)^2(k^2 + 4k + 4)}{4}$ — expand
6) $= \frac{(k+1)^2(k+2)^2}{4}$ — factor/math
7) $= \frac{(k+1)^2((k+1)+1)^2}{2}$ — math

8) P(k+1) is true

4

Def'n of P(n)

6. Prove that $11^n - 6$ is divisible by 5 for every positive integer n.

Conclusion: Since assuming P(k) leads to P(k+1), I have shown P(k) → P(k+1) for k ∈ ℤ⁺. I have completed the inductive step.

Conclusion: Since the base case and inductive steps are true, I have proven P(n) is true for n ∈ ℤ⁺ by mathematical induction.

Base case: look at P(1):

$\boxed{\text{get to } 11^{k+1} - 6 = 5S}$

$11^1 - 6$ is divisible by 5

5 is divisible by 5

∴ 5 is divisible by 5, therefore P(1) is true and thus the base case is true.

ind hyp: P(k) : $11^k - 6$ is div. by 5, $k \in \mathbb{Z}^+$

1) $5 \mid 11^k - 6$ — assume P(k)

2) $11^k - 6 = 5t,\ t \in \mathbb{Z}$ — def'n of div.

3) $11^k = 5t + 6$ — math

4) $11^k \cdot 11 = 11(5t + 6)$ — multiply both sides by 11

5) $11^{k+1} = 11(5t+6)$ — math

6) $11^{k+1} = 55t + 66$ — math

7) $11^{k+1} - 6 = 55t - 66 - 6$ — sub. 6 both sides

8) $11^{k+1} - 6 = 55t - 60$ — math

9) $11^{k+1} - 6 = 5(11t + 12)$ — math

10) $S = 11t + 12,\ S \in \mathbb{Z}$ — def'n new variable

11) $11^{k+1} - 6 = 5S$ — sub S

12) $5 \mid 11^{k+1} - 6$ — def'n of divisibility

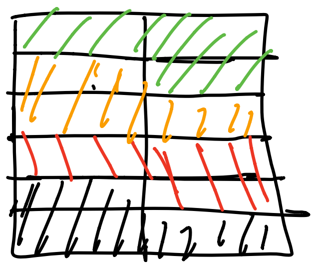
13) $P(k+1)$ — def'n of P(n)

Conc: As shown, if P(k) is true then P(k+1) is true. ...

7. Prove that a 6×2^n checkerboard can be completely covered using right triominoes for every positive integer n.

Base case: 6×2

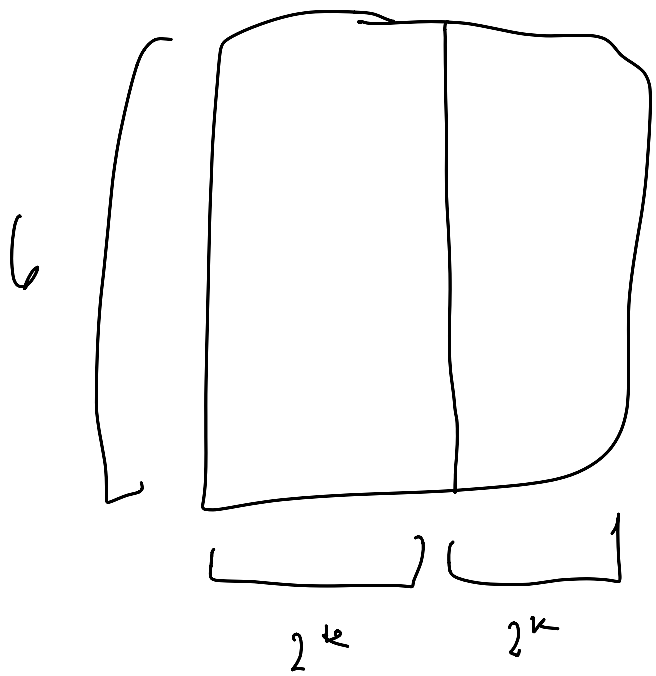
↑ rows



I have shown a 6×2 checkerboard can be completely filled by right triominoes.

Therefore $P(1)$ is true, base case holds

Induc Hyp: assume $P(k)$: 6×2^k checker board can be tiled



$2^{k+1} = 2(2^k)$

we know by ind. hyp we can tile 6×2^k checkerboard. Putting 2 6×2^k checkerboards side by side gives a $6\times2^{k+1}$ checkerboard. So we can tile a $6\times2^{k+1}$ checkerboard

Thus $P(k+1)$ is true

finish