HW3 Math 350 Joseph Schmidt

2. $d = \gcd(15, 6)$

$d = 3$

$3 \nmid 8$

$\therefore$ According to Theorem 3.23
this linear diophantine equation has no solutions

2. $24x + 35y = 94$

a) $d = \gcd(24, 35) = 1$

$1 \mid 94$, there exists infinitely many solutions

b) $35 = 24 \cdot 1 + 11$ $\quad 35 - 24 = 11$
$24 = 11 \cdot 2 + 2$
$24 + 11(-2) = 2$

$47(24 + 11(-2)) = 2$
$47 \cdot 24 + 47(35 + 24(-1))(-2) = 94$
$47 \cdot 24 + 47 \cdot 35(-2) + 47 \cdot 2 \cdot 24 = 94$
$141 \cdot 24 + (-94) \cdot 35 = 94$

$x = 141 \quad y = -94$

c) $x = 141 + 35n \quad y = -94 - 24n$

from
$x = x_0 + \left(\frac{b}{d}\right)n \quad y = y_0 - \left(\frac{a}{d}\right)n$

d being 1 in this case from $d = \gcd(35, 24)$

$x = 141 + 35n \quad y = -94 - 24n$

$-94 - 24n > 0$

$-94 > 24n$

$-3.91 > n$

$141 + 35n > 0$

$141 > -35n$

$-4.02 < n$

d)

$-4.02 < n < -3.91$

$n = -4$, n is an integer and -4 is the only integer that satisfies inequality

$x = 141 + 35(-4) \quad y = -94 - 24(-4)$

$x = 1 \quad y = 2$

$24(1) + 35(2) = 94$

3. Base case: $n=2$, $2^{2^2} = 2^4 = 16$

Induction step: $2^{2^{n+1}} = 2^{2^n \cdot 2} = (2^{2^n})^2$

Take $2^{2^n} = 10k+6$

Then $(2^{2^n})^2 = (10k+6)^2$

$= (10k+6)(10k+6)$

$= 100k^2 + 120k + 36$

These two terms will not contribute to ones place as they are divisible by 10.

So 36 only number to contribute which has 6 in its place.

$(1\times10^2 + 0\times10^1 + 0\times10^0)k^2 + (1\times10^2 + 2\times10^1 + 0\times10^0)k + 3\times10^1 + 6\times10^0$

$k^2\times10^2 + k\times10^2 + 2k\times10^1 + 3\times10^2 + \underbrace{6\times10^0}$

only term contributing to the 1s place

$F_n = 2^{2^n} + 1$

For $n \geq 2$ use induction we proved prior

$$F_n = \underbrace{k^2 \times 10^2 + k \times 10^2 + 2k \times 10^2 + 3 \times 10^1 + 6 \times 10^0}_{=} + \underbrace{7 \times 10^0}_{\text{only number contributing to the one's place}} + 1 \times 10^0$$

---

4. $47 \bmod 23 = 1 \bmod 23$ [step 1

$\therefore 47 \equiv 1 \pmod{23}$ theorem 4.3

step 2

$47 \equiv 1 \equiv 1 \pmod{23}$ definition of congruence

$47^{18} \equiv 1^{18} \pmod{23} \equiv 1^{18}$ theorem 4.8

$1^{18} \equiv 1 \equiv 1 \pmod{23}$

so,

$47^{18} \equiv 1^{18} \equiv 1 \pmod{23}$

---

step 3

$47 \equiv 1 \pmod{23}$

$47 - 23 \equiv 1 \pmod{23}$ Definition of mod

$24 \equiv 1 \pmod{23}$

$24 + 2 \equiv 1 + 2 \pmod{23}$ Theorem 4.4

$26 \equiv 3 \pmod{23}$

Step 4

$26 \equiv 3 \pmod{23} \equiv 3$ Theorem 4.2

$26^{12} = 3^{12} \pmod{23} \equiv 3^{12}$ Theorem 4.8

$3^{12} = 3 + 23 \cdot 106 \ (23)$ Theorem 4.1

$\Rightarrow 3^{12} \equiv 3 \pmod{23}$

$3^{12} = (3^3)^4 = 27^4$

$\Rightarrow 27^4 \equiv 3^{12} \equiv 3 \pmod{23}$

$4^4 = 3 + 23 \ (11)$

$\Rightarrow 4^4 \equiv 3 \pmod{23}$

Step 5

$47^{18} \equiv 1 \pmod{23}$ from earlier parts

$26^{12} \equiv 3 \pmod{23}$

$47^{18} + 26^{12} \equiv 1 + 3 \pmod{23}$ Theorem 4.4

$47^{18} + 26^{12} \equiv 4 \pmod{23}$

5. $d = \gcd(a, m)$

$d = \gcd(12, 20)$

$d = 4$

$4 \mid 8$

$\therefore 12x \equiv 8 \pmod{20}$, has 4 incongruent solutions

$ax - my = b$

$12x - 20y = 8$

$x = -1 \quad y = -1$

$x = -1 + \left(\frac{20}{4}\right)t = -1 + 5t$

$t = 0 \Rightarrow -1 + 0 = -1$

$t = 1 \Rightarrow -1 + 5 = 4$

$t = 2 \Rightarrow -1 + 10 = 9$

$t = 3 \Rightarrow -1 + 15 = 14$

$14 - -1 = 15 + 5 = 20$, wraps back around

$\therefore x = -1, 4, 9, 14$ is a set of incongruent solutions

6. $n = n \cdot k + r \quad k \geq 2$

Say it could

$n = n \cdot k + 2$

$a \equiv 2 \pmod 4$
$a^a \equiv 2^a \pmod 4$

$2 = 2a + 4 \qquad a \equiv 2 \pmod 4 \equiv 2$
$1 = a + 2 \qquad b^3 \equiv 2 \pmod 4 \equiv 2$
$-1 = a$

$n^n = (mq + n)^n$

$2^k \pmod 4$ where $k \geq 2$
show that it is never 2

2^{n+2}
$4 \cdot 2^n \pmod 4$

$m \mid b \therefore$

$k \geq 2$
$\Rightarrow k = \varepsilon + 2$ for some $\varepsilon \geq 0$
$\Rightarrow n \equiv r \pmod 4$
$\Rightarrow n^k \equiv r^k \pmod 4$
Take $r = 2$
$\Rightarrow n^k = 2^k \pmod 4$
$\Rightarrow n^k = 2^{\varepsilon+2} \pmod 4$
$\Rightarrow n^k = 2^\varepsilon \cdot 2^2 \pmod 4$
$\Rightarrow n^k = 4 \cdot 2^\varepsilon \pmod 4$
$\therefore m \mid b$
meaning for $k \geq 2$ $r \neq 2$