

$$1. (a) \quad 306 = 84 \cdot \underline{3} + \underline{54}$$

$$84 = 54 \cdot \underline{1} + \underline{30}$$

$$54 = 30 \cdot \underline{1} + \underline{24}$$

$$30 = 24 \cdot \underline{1} + \underline{6}$$

$$24 = 6 \cdot \underline{4} + \underline{0}$$

last nonzero remainder is  $\gcd(306, 84)$ .

$$(b) \quad 51 = 14 \cdot \underline{3} + \underline{9}$$

$$14 = 9 \cdot \underline{1} + \underline{5}$$

$$9 = 5 \cdot \underline{1} + \underline{4}$$

$$5 = 4 \cdot \underline{1} + \underline{1}$$

$$\text{or} \quad r_2 = 9 = 51 - (14)(3) = r_0 - 3r_1$$

$$\text{or} \quad r_3 = 5 = 14 - 9 = r_1 - r_2$$

$$\text{or} \quad r_4 = 4 = 9 - 5 = r_2 - r_3$$

$$\text{or} \quad \gcd(51, 14) = 1 = 5 - 4 = r_3 - r_4$$

To reassemble, we have

$$\gcd(51, 14) = r_3 - r_4 = r_3 - (r_2 - r_3) = 2r_3 - r_2$$

$$= 2(r_1 - r_2) - r_2 = 2r_1 - 3r_2 = 2r_1 - 3(r_0 - 3r_1)$$

$$= 11r_1 - 3r_0, \text{ or } 1 = 51s + 14t \text{ with } s = -3, t = 11.$$

(c) Each of 84, 54, and 306 is divisible by 6. So

$$84x \equiv 54 \pmod{306} \quad \text{gives way to } 14x \equiv 9 \pmod{51}.$$

From part (b), we deduce 11 is the multiplicative inverse of 14 in  $\mathbb{Z}_{51}$ .

$$\text{So, } x \equiv (11)(14x) \equiv (11)(9) \equiv 48 \pmod{51}.$$

In the integers

$$48, 99, 150, 201, 252, 303, 354, 405, \dots$$

are all equivalent mod 51. Back in mod 306, there is no redundancy

until you reach 354. Thus

$$x \equiv 48, 99, 150, 201, 252, 303 \pmod{306}$$

2.  $\underline{49} = 7^2$ ,  $\underline{93} = 31 \cdot 3$ ,  $\underline{119} = 17 \cdot 7$ , so these three are not prime.

But no prime number less than  $\sqrt{67}$  divides  $\underline{67}$

no prime number less than  $\sqrt{71}$  divides  $\underline{71}$

no prime number less than  $\sqrt{193}$  divides  $\underline{193}$

} so these three are primes

3. (a) 71 is prime (see above), and  $71 \nmid 68$ . Thus, by Fermat's Little Theorem,

$$68^{70} \equiv 1 \pmod{71}, \text{ and } 68^{71} \equiv 68 \pmod{71}$$

$$\begin{aligned} \text{So, } 68^{712} &= 68^{710} \cdot 68^2 = (68^{71})^{10} \cdot 68^2 \equiv (68)^{10} \cdot 68^2 \\ &\equiv (-3)^{12} \equiv (3^4)^3 = 81^3 \equiv 10^3 = 1000 \equiv 6 \pmod{71}. \end{aligned}$$

$$\text{This means } 68^{712} \pmod{71} = \boxed{6}$$

(b)  $49 = 7^2$  and  $85 = 5 \cdot 17$ , so  $\gcd(49, 85) = 1$ , meaning that Euler's Theorem applies.  $\phi(85) = \phi(5)\phi(17) = (4)(16) = 64$ .

$$\text{So } 49^{64} \equiv 1 \pmod{85}. \text{ Hence}$$

$$\begin{aligned} 49^{642} &= 49^{640} \cdot 49^2 = (49^{64})^{10} \cdot 49^2 \equiv 1^{10} \cdot 49^2 \\ &= 7^3 \cdot 7 = 343 \cdot 7 \equiv 3 \cdot 7 \equiv 21 \pmod{85}. \end{aligned}$$

$$\text{Hence } 49^{642} \pmod{85} = \boxed{21}$$

$$4. (a) \phi(42) = \phi(7)\phi(3)\phi(2) = 6 \cdot 2 \cdot 1 = \boxed{12}$$

$$(b) \phi(45^3) = \phi(3^6 \cdot 5^3) = 3^6 \cdot 5^3 \cdot (1 - \frac{1}{3})(1 - \frac{1}{5}) = 48600$$

5. (a) This recurrence is  $2^{\text{nd}}$  degree, and only requires two initial values.

$$a_0 = 0, \quad a_1 = 0.$$

$$(b) \quad a_2 = 2a_1 + a_0 + 2 \cdot 3^0 = 2$$

$$a_3 = 2a_2 + a_1 + 2 \cdot 3^1 = (2)(2) + 0 + 6 = 10$$

$$a_4 = 2a_3 + a_2 + 2 \cdot 3^2 = (2)(10) + 2 + 18 = 40$$

$$a_5 = 2a_4 + a_3 + 2 \cdot 3^3 = (2)(40) + 10 + 54 = 144$$

$$a_6 = 2a_5 + a_4 + 2 \cdot 3^4 = (2)(144) + 40 + 162 = \boxed{490}$$

6. Substituting  $r^n$  for  $a_n$  ( $r^{n-1}$  for  $a_{n-1}$ ,  $r^{n-2}$  for  $a_{n-2}$ ) takes us from

$$a_n - 7a_{n-1} + 10a_{n-2} = 0 \quad \text{to} \quad r^2 - 7r + 10 = 0$$

$$\text{or} \quad (r-5)(r-2) = 0 \quad \Rightarrow \quad r = 2, 5.$$

Terms in the sequence are a weighted sum of  $2^n$  and  $5^n$ :

$$a_n = \alpha_1 \cdot 2^n + \alpha_2 \cdot 5^n.$$

Our initial values give

$$2 = a_0 = \alpha_1 \cdot 2^0 + \alpha_2 \cdot 5^0 = \alpha_1 + \alpha_2$$

$$1 = a_1 = \alpha_1 \cdot 2^1 + \alpha_2 \cdot 5^1 = 2\alpha_1 + 5\alpha_2$$

These 2 equations in unknown weights  $\alpha_1, \alpha_2$

$$\left. \begin{array}{l} \alpha_1 + \alpha_2 = 2 \\ 2\alpha_1 + 5\alpha_2 = 1 \end{array} \right\} \text{ can be solved to obtain } \begin{array}{l} \alpha_1 = 3 \\ \alpha_2 = -1 \end{array}$$

So, the solution is

$$a_n = 3 \cdot 2^n - 5^n$$

7. (a) Here,  $a=3$ ,  $b=2$ ,  $c=1$  and  $d=2$ , which means  $a < b^d$ . Thus,

$$T(n) \text{ is } O(n^2).$$

(b) This time,  $a=4$ ,  $b=2$ ,  $c=\frac{1}{2}$ ,  $d=1$ , so  $a > b^d$ . Thus,

$$g(n) \text{ is } O(n^{\log_2 4}) = O(n^2) \text{ again.}$$

8. Base step: The sum of digits in  $\lambda$  is 0 and  $3|0$

The sum of digits in "27" is 9 and  $3|9$

The sum of digits in "9" is 9 and  $3|9$

The sum of digits in "414" is 9 and  $3|9$

Induction step: Our new word  $w = w_1 w_2$  is the concatenation of words  $w_1, w_2$  and, by the induction hypothesis,  $w_1$  and  $w_2$  satisfy the claim.

Since the sum of digits in  $w$  is merely the sum of digits in  $w_1$  plus the sum of digits in  $w_2$ , and since the sum of any two numbers both divisible by 3 is again divisible by 3, it follows that  $w$  also satisfies the claim.