DMTH237 Discrete Mathematics II — Assignment 5

Christian Nassif-Haynes

May 31, 2013

1. (a) The complementary function is
$$a_n^{(c)} = c_1 4^n + c_2 3^n.$$
For a particular solution, let us try
$$a_n^{(p)} = A2^n.$$
Then
$$a_{n+1}^{(p)} = A2^{n+1} = 2A2^n$$
and
$$a_{n+2}^{(p)} = A2^{n+2} = 4A2^n.$$
It follows that
$$a_{n+2}^{(p)} - 7a_{n+1}^{(p)} + 12a_n^{(p)} = (4A - 14A + 12A)2^n = 2A2^n = 2^n$$
if $A = \frac{1}{2}$. Hence
$$a_n = a_n^{(c)} + a_n^{(p)} = c_1 4^n + c_2 3^n + 2^{n-1}.$$

   (b) The complementary function is
$$a_n^{(c)} = c_1 4^n + c_2 3^n.$$
For a particular solution, let us try
$$a_n^{(p)} = A_0 + A_1 n + A_2 n^2.$$
Then
$$a_{n+1}^{(p)} = A_0 + A_1(n+1) + A_2(n+1)^2 = A_0 + A_1 + A_2 + A_1 n + 2A_2 n + A_2 n^2$$
and
$$a_{n+2}^{(p)} = A_0 + A_1(n+2) + A_2(n+2)^2 = A_0 + 2A_1 + 4A_2 + A_1 n + 4A_2 n + A_2 n^2.$$
It follows that
$$a_{n+2}^{(p)} - 7a_{n+1}^{(p)} + 12a_n^{(p)} = (6A_0 - 5A_1 - 3A_2) + (6A_1 - 10A_2)n + 6A_2 n^2 = n^2$$
if $A_0 = \frac{17}{54}$, $A_1 = \frac{5}{18}$ and $A_2 = \frac{1}{6}$. Hence
$$a_n = a_n^{(c)} + a_n^{(p)} = c_1 4^n + c_2 3^n + \frac{17}{54} + \frac{5}{18}n + \frac{1}{6}n^2.$$

   (c) The complementary function is
$$a_n^{(c)} = c_1 4^n + c_2 3^n.$$
For a particular solution, let us try
$$a_n^{(p)} = (B_0 + B_1 n + B_2 n^2)B2^n = (A_0 + A_1 n + A_2 n^2)2^n.$$
Then
$$a_{n+1}^{(p)} = \left(A_0 + A_1(n+1) + A_2(n+1)^2\right)2^{n+1} = (2A_0 + 2A_1 + 2A_2 + 2A_1 n + 4A_2 n + 2A_2 n^2)2^n$$
and
$$a_{n+2}^{(p)} = \left(A_0 + A_1(n+2) + A_2(n+2)^2\right)2^{n+2} = (4A_0 + 8A_1 + 16A_2 + 4A_1 n + 16A_2 n + 4A_2 n^2)2^n.$$

It follows that

$$a_{n+2}^{(p)} - 7a_{n+1}^{(p)} + 12a_n^{(p)} = \left((2A_0 - 6A_1 + 2A_2) + (2A_1 - 12A_2)n + 2A_2n^2\right)2^n = n^2 2^n$$

if $A_0 = \frac{17}{2}$, $A_1 = 3$ and $A_2 = \frac{1}{2}$. Hence

$$a_n = a_n^{(c)} + a_n^{(p)} = c_1 4^n + c_2 3^n + \frac{17}{2} + 3n + \frac{1}{2}n^2.$$

(d) The complementary function is

$$a_n^{(c)} = c_1 2^n.$$

For a particular solution, let us try

$$a_n^{(p)} = A_0 \cos n + A_1 \sin n.$$

Then

$$a_{n+1}^{(p)} = A_0 \cos(n+1) + A_1 \sin(n+1).$$

It follows that

$$a_{n+1}^{(p)} - 2a_n^{(p)} = (A_0 \cos 1 - 2A_0 + A_1 \sin 1)\cos n + (-A_0 \sin 1 - 2A_1 + A_1 \cos 1)\sin n = \cos n$$

if

$$A_0 = -\frac{\cos 1 - 2}{4\cos 1 - 5} \qquad \text{and} \qquad A_1 = \frac{\sin 1}{5 - 4\cos 1}.$$

Hence

$$a_n = a_n^{(c)} + a_n^{(p)} = c_1 2^n + \frac{\cos 1 - 2}{5 - 4\cos 1}\cos n + \frac{\sin 1}{5 - 4\cos 1}\sin n.$$

(e) The complementary function is

$$a_n^{(c)} = c_1 + c_2 5^n.$$

For a particular solution, let us try

$$a_n^{(p)} = A_0 + A_1 n.$$

Then

$$a_{n+1}^{(p)} = A_0 + A_1(n+1) = A_0 + A_1 + A_1 n$$

and

$$a_{n+2}^{(p)} = A_0 + A_1(n+2) = A_0 + 2A_1 + A_1 n.$$

But

$$a_{n+2}^{(p)} - 7a_{n+1}^{(p)} + 12a_n^{(p)} = (-4A_1) + (0)n \neq n.$$

Now we try

$$a_n^{(p)} = A_0 n + A_1 n^2.$$

Then

$$a_{n+1}^{(p)} = A_0(n+1) + A_1(n+1)^2 = (A_0 + A_1) + (A_0 + 2A_1)n + A_1 n^2$$

and

$$a_{n+2}^{(p)} = A_0(n+2) + A_1(n+2)^2 = (2A_0 + 4A_1) + (A_0 + 4A_1)n + A_1 n^2.$$

It follows that

$$a_{n+2}^{(p)} - 6a_{n+1}^{(p)} + 5a_n^{(p)} = (-4A_0 - 2A_1) - 8A_1 n = n$$

if $A_0 = \frac{1}{16}$ and $A_1 = -\frac{1}{8}$. Hence

$$a_n = a_n^{(c)} + a_n^{(p)} = c_1 + c_2 5^n + \frac{1}{16}n + \frac{1}{8}n^2.$$

2. (a) We have

$$a_n = 2a_{n-1} + 2^n - 1 \tag{1}$$

with initial condition $a_0 = 0$. Rewriting and multiplying throughout by X^n, we obtain

$$a_{n+1}X^n - 2a_nX^n = \left(2^{n+1} - 1\right)X^n.$$

Summing over $n = 0, 1, 2, \ldots$ and multiplying throughout again by X, we obtain

$$X\sum_{n=0}^{\infty} a_{n+1}X^n - 2X\sum_{n=0}^{\infty} a_nX^n = X\sum_{n=0}^{\infty}\left(2^{n+1} - 1\right)X^n.$$

It follows that

$$(G(X) - a_0) - 2XG(X) = XF(X) \tag{2}$$

where

$$F(X) = \sum_{n=0}^{\infty}\left(2^{n+1} - 1\right)X^n$$

is the generating function of the sequence $2^{n+1} - 1$. The generating function of the sequence 2^{n+1} is

$$F_1(X) = 2 + 4X + 8X^2 + \ldots = 2(1 + 2X + 4X^2 + \ldots) = \frac{2}{1 - 2X},$$

while the generating function of the sequence $-1 = -(1^n)$ is

$$F_2(X) = -1 - 1 - 1 - \ldots = -(1 + 1 + 1 + \ldots) = -\frac{1}{1 - X}.$$

We therefore have

$$F(X) = F_1(X) + F_2(X) = \frac{2}{1 - 2X} - \frac{1}{1 - X}. \tag{3}$$

On the other hand, substituting the initial conditions into (2) and combining with (3), we have

$$G(X)(1 - 2X) = \frac{2X}{1 - 2X} - \frac{X}{1 - X}$$

which can be expressed as partial fractions in the form

$$G(X) = \frac{1}{(1 - 2X)^2} - \frac{2}{1 - 2X} + \frac{1}{1 - X}.$$

It follows from the extended binomial theorem that the solution to the given recurrence relation in (1) is

$$a_n = 2^n(n + 1) - 2 \cdot 2^n + 1 = n2^n - 2^n + 1$$

(b) We have

$$t_{2^m} = a_m$$

so that

$$t_m = a_{\log_2 m} = (\log_2 m)2^{\log_2 m} - 2^{\log_2 m} + 1 = m\log_2 m - m + 1.$$

Now, for large m the terms in $-m + 1$ become negligible so that

$$t_m = O(m\log_2 m) \qquad \text{as } m \to \infty.$$

In other words $t_n \sim n\log_2 n$ for large n.

3. The 28-state machine

$$\text{INC} + \text{INC} + \text{INC} + \text{INC} + \text{INC} + \text{EXP},$$

which we will name M is as follows.

	0	**1**
0	1R1	1L0
1	2R2	2L1
2	3R3	3L2
3	4R4	4L3
4	5R5	5L4
5	EXP	
⋮		
27		

When started on a blank tape, the first five states, which comprise the machine

$$\text{INC} + \text{INC} + \text{INC} + \text{INC} + \text{INC},$$

will set $n = 5$. Now EXP will be run with $n = 5$ so that $m = 2^{2^{2^{2^{2}}}}$ is calculated.

In calculating m, EXP must write at least m 1's to the tape, each time having to perform at least one step. Also, since INC and EXP both halt M does too. Therefore,

$$\beta(28) \geq 2^{2^{2^{2^{2}}}} > 2 \times 10^{19728}.$$

4. (a) We will use the extended Euclidean algorithm and work backwards to find an expression of the form $1 = ax + by$. We have

$$\begin{aligned} 211 \div 135 &= 1\,\mathrm{r}\,76, \\ 135 \div 76 &= 1\,\mathrm{r}\,59, \\ 76 \div 59 &= 1\,\mathrm{r}\,17, \\ 59 \div 17 &= 3\,\mathrm{r}\,8, \\ 17 \div 8 &= 2\,\mathrm{r}\,1 \end{aligned}$$

so that

$$\begin{aligned} 1 &= 17 - 8 \times 2, && \text{(working backwards)} \\ &= 17 - (59 - 17 \times 3) \times 2, && \text{(working backwards)} \\ &= 17 \times 7 - 59 \times 2, && \text{(collecting like terms)} \\ &= (76 - 59) \times 7 - 59 \times 2, && \text{(working backwards)} \\ &= 76 \times 7 - 59 \times 9, && \text{(collecting like terms)} \\ &= 76 \times 7 - (135 - 76) \times 9, && \text{(working backwards)} \\ &= 76 \times 16 - 135 \times 9, && \text{(collecting like terms)} \\ &= (211 - 135) \times 16 - 135 \times 9, && \text{(working backwards)} \\ &= 211 \times 16 - 135 \times 25. && \text{(collecting like terms)} \end{aligned}$$

Thus the inverse of 135 modulo 211 is $-25 \equiv 186$.

(b) We have

$$\begin{aligned} 27^{68} &\equiv (-4)^{68} \mod 31 \\ &= 4^{2\times(31-1)+8} = (4^{30})^2 \times 4^8 \\ &\equiv 1^2 \times 4^8 \mod 31 && \text{(by Fermat's little theorem)} \\ &= 4^{3^2} \times 4^2 = 64^2 \times 4^2 \\ &\equiv 2^2 \times 4^2 \mod 31 \\ &= 4^3 = 64 \\ &\equiv 2 \mod 31. \end{aligned}$$

(c) Using Euler's totient function yields

$$\varphi(48) = \varphi(2^4 \times 3) = 48\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 16$$

so that

$$\begin{aligned}
(11^{16})^{300} \times 11^5 &\equiv 1^{300} \times 11^5 \mod 48 \\
&= (11^2)^2 \times 11 \\
&\equiv (25)^2 \times 11 \mod 48 \\
&= (5 \times 5)^2 \times 11 = 5^2 \times 5 \times 55 \\
&\equiv 5^2 \times 5 \times 7 \mod 48 \\
&\equiv 11 \mod 48.
\end{aligned}$$

(d) Applying Wilson's theorem we find

$$38! = \frac{(41-1)!}{39 \times 40} \equiv \frac{-1}{39 \times 40} \mod 41$$

so that what is left is to solve the linear congruence equation

$$-39 \times 40x \equiv 1 \mod 41$$

for $x \in \mathbb{N}$. Noting that $-40 \equiv 1$ modulo 41 we obtain the reduced equation

$$39x \equiv 1 \mod 41.$$

Now x is the inverse of 39 modulo 41 so we can use the extended Euclidean algorithm. We have

$$\begin{aligned}
41 \div 39 &= 1 \,\mathrm{r}\, 2, \\
39 \div 2 &= 19 \,\mathrm{r}\, 1
\end{aligned}$$

so that, by back substitution,

$$\begin{aligned}
1 &= 39 - 19 \times 2 \\
&= 39 - 19 \times (41 - 39) \\
&= 39 \times 20 - 19 \times 41.
\end{aligned}$$

Therefore the remainder of $38! \div 41$ is 20.

5. (a) The encoded message is

$$m' \equiv 31^{17} \equiv 633511 \mod 746003.$$

(b) Seeing as $\varphi(n_E) = \varphi(746003)$ divides $e_E d_E - 1 = 17 \times 218873 - 1$, we must have

$$e_E d_E - 1 = k\varphi(n_E) = k(p-1)(q-1)$$

for some $k \in \mathbb{Z}$. Now, as $\varphi(n) < n$ and $\varphi(n) \approx n$ for large n, we have

$$k > \frac{e_E d_E - 1}{n_E} = \frac{3720840}{746003} \approx 4.99.$$

Hence, let us try $k = 5$, which gives

$$(p-1)(q-1) = \frac{3720840}{5} = 744168. \tag{4}$$

Combining $pq = n_E = 746003$ with (4) we see that one solution is

$$p = 607 \qquad \text{and} \qquad q = 1229.$$

(c) Using the primes found in the previous part we have

$$\varphi(746003) = 746003\left(1 - \frac{1}{607}\right)\left(1 - \frac{1}{1229}\right) = 744168.$$

(d) The decoding key for Alice is the multiplicative inverse of 7 modulo $\varphi(746003) = 744168$. Applying the extended Euclidean algorithm we find

$$\begin{aligned} 744168 \div 7 &= 106309\,\mathrm{r}\,5, \\ 7 \div 5 &= 1\,\mathrm{r}\,2 \\ 5 \div 2 &= 2\,\mathrm{r}\,1 \end{aligned}$$

so that

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - (7 - 5) \times 2 \\ &= 5 \times 3 - 7 \times 2 \\ &= (744168 - 106309 \times 7) \times 3 - 7 \times 2 \\ &= 744168 \times 3 - 7 \times 318929 \end{aligned}$$

Therefore, Alice's decoding key is $-318929 \bmod 744168 = 425239$.

(e) Reducing $242435^{425239} \bmod 746003$ we see that the original message is 23517.

[bonus marks]

Seeing as $\varphi(m)$ divides $1019 \times 136859 - 1 = 139459320$, we must have

$$139459320 = k(p-1)(q-1)$$

for some $k \in \mathbb{Z}$. Now, as $\varphi(m) < m$ and $\varphi(m) \approx m$ for large m, we have

$$k > \frac{139459320}{m} = \frac{139459320}{295927} \approx 471.26.$$

Hence, let us try $k = 472$, which gives

$$(p-1)(q-1) = \frac{139459320}{472} \approx 295464.66.$$

Then $k = 473$,

$$\varphi(m) = (p-1)(q-1) = \frac{139459320}{473} = 294840. \tag{5}$$

Combining $pq = 295927$ with (5) we see that the solution is

$$p = 541 \qquad \text{and} \qquad q = 547.$$

Now, the decoding exponent is the multiplicative inverse of 11 modulo $\varphi(m)$, which is 80411. The reader is encouraged to fill in the details here as the author is feeling sleepy.

Reducing 227687^{80411} modulo 295927 by computer yields 53110. Proceeding similarly with the remaining groups of digits yields the decrypted message

53110, 6866, 10012, 3611, 5085, 20094, 20859, 27689, 24015, 39755. 21167, 51240.

Converting the first group from decimal to base-41, we have the sequence 31 24 15—that is, T M D. Performing the conversion on the other groups using the code in appendix A we come to the conclusion that

`DMTH237:42510023: TEACHES COOL MATHS`

with the first colon at $k = 8$, assuming the initial 'D' is the $k = 1^{\text{st}}$ character. Notice that in decoding the message we had to reverse the characters T M D, along with the characters in the other groups.

A Code Listing

The code used to convert from base-10 to base-41, written in Python 3, is show below.

```
def str (number):
   chars = "0123456789 ABCDEFGHIJKLMNOPQRSTUVWXYZ,:."

   result = ''
   while number != 0:
      number, rdigit = divmod(number, 41)
      result = result + chars[rdigit-1]

   return result

def msg ():
   decoded = [53110, 6866, 10012, 3611, 5085, 20094,
             20859, 27689, 24015, 39755, 21167, 51240]
   for n in decoded:
      print(str(n), end = "")
```