Solutions to MATH3411 Problems 76–83

76. We first factor $n = 8051$:

		$\gcd(x_{2i} - x_i, n)$
$x_0 \equiv 1$		
$x_1 \equiv 2$		
$x_2 \equiv 5$	$x_2 - x_1 \equiv 3$	1
$x_3 \equiv 26$		
$x_4 \equiv 677$	$x_4 - x_2 \equiv 672$	1
$x_5 \equiv 7474$		
$x_6 \equiv 2839$	$x_6 - x_3 \equiv 2813$	97

We have found a factor $d = 97$. It is a prime and so is $\dfrac{n}{d} = 83$, so $n = 91643 = 83 \times 97$.
Now let us factor $n = 201001$:

		$\gcd(x_{2i} - x_i, n)$
$x_0 \equiv 1$		
$x_1 \equiv 2$		
$x_2 \equiv 5$	$x_2 - x_1 \equiv 3$	1
$x_3 \equiv 26$		
$x_4 \equiv 677$	$x_4 - x_2 \equiv 672$	1
$x_5 \equiv 56328$		
$x_6 \equiv 42800$	$x_6 - x_3 \equiv 42774$	1
$x_7 \equiv 117888$		
$x_8 \equiv 170404$	$x_8 - x_4 \equiv 169727$	19

We have found a prime factor $d = 19$ of $n = 201001$.

We now factor the quotient $\dfrac{n}{d} = 10579$:

		$\gcd(x_{2i} - x_i, n)$
$x_0 \equiv 1$		
$x_1 \equiv 2$		
$x_2 \equiv 5$	$x_2 - x_1 \equiv 3$	1
$x_3 \equiv 26$		
$x_4 \equiv 677$	$x_4 - x_2 \equiv 672$	1
$x_5 \equiv 3433$		
$x_6 \equiv 484$	$x_6 - x_3 \equiv 458$	1
$x_7 \equiv 1519$		
$x_8 \equiv 1140$	$x_8 - x_4 \equiv 463$	1
$x_9 \equiv 8963$		
$x_{10} \equiv 9023$	$x_{10} - x_5 \equiv 5590$	1
$x_{11} \equiv 9125$		
$x_{12} \equiv 8896$	$x_{12} - x_6 \equiv 8412$	1
$x_{13} \equiv 7897$		
$x_{14} \equiv 9984$	$x_{14} - x_7 \equiv 8465$	1
$x_{15} \equiv 4919$		
$x_{16} \equiv 2389$	$x_{16} - x_8 \equiv 1249$	1
$x_{17} \equiv 5241$		
$x_{18} \equiv 4998$	$x_{18} - x_9 \equiv 6614$	1
$x_{19} \equiv 2986$		
$x_{20} \equiv 8679$	$x_{20} - x_{10} \equiv 10235$	1
$x_{21} \equiv 2562$		
$x_{22} \equiv 4865$	$x_{22} - x_{11} \equiv 6319$	71

We have found another prime factor $d = 71$, and the quotient $\dfrac{201001}{19 \times 71} = 149$ is also prime, so $n = 201001 = 19 \times 71 \times 149$.

77. Let us now first use Fermat's Method: For $n = 92131$, $\lceil \sqrt{n} \rceil =$, so

t	$2t+1$	$s^2 = t^2 - n$	$s \in \mathbb{Z}$?
304	609	285	×
305	611	894	×
306	613	1505	×
307	615	2118	×
308	617	2733	×
309	619	3350	×
310	621	3969	✓

so $t = 310$ and $s = \sqrt{3969} = 63$, and $a = s+t = 373$ and $b = t-s = 247$; hence, $92131 = n = ab = 373 \times 247$. The number 373 is prime but 247 is not; we need to factorise the latter: $\lceil \sqrt{247} \rceil = 16$, so

t	$2t+1$	$s^2 = t^2 - n$	$s \in \mathbb{Z}$?
16	33	9	✓

so $t = 16$ and $s = \sqrt{9} = 3$, and $a = s + t = 19$ and $b = t - s = 13$; these are prime factors, so $92131 = 13 \times 19 \times 373$.

Let us now use the Pollard ρ-Method:

		$\gcd(x_{2i} - x_i, n)$
$x_0 \equiv 2$		
$x_1 \equiv 5$		
$x_2 \equiv 26$	$x_2 - x_1 \equiv 21$	1
$x_3 \equiv 677$		
$x_4 \equiv 89806$	$x_4 - x_2 \equiv 89780$	1
$x_5 \equiv 62028$		
$x_6 \equiv 82225$	$x_6 - x_3 \equiv 81548$	19

We have found a factor $d = 19$ and factor the quotient $\frac{n}{d} = 4849$:

		$\gcd(x_{2i} - x_i, n)$
$x_0 \equiv 2$		
$x_1 \equiv 5$		
$x_2 \equiv 26$	$x_2 - x_1 \equiv 21$	1
$x_3 \equiv 677$		
$x_4 \equiv 2524$	$x_4 - x_2 \equiv 2498$	1
$x_5 \equiv 3840$		
$x_6 \equiv 4641$	$x_6 - x_3 \equiv 3964$	1
$x_7 \equiv 4473$		
$x_8 \equiv 756$	$x_8 - x_4 \equiv 3081$	13

We have found another prime factor $d = 13$, and $\frac{92131}{19 \times 13} = 373$ is also prime, so $n = 92131 = 13 \times 19 \times 373$.
Finally, we use Shor's Algorithm on $n = 92131$: $3^{558} \equiv 1 \pmod{n}$, so $n|(3^{558} - 1) = (3^{279} - 1)(3^{279} + 1)$.
Now, it is possible to calculate $\gcd(n, 3^{279} - 1) = 13$ and $\gcd(n, 3^{279} + 1) = 7087$ to find the factors 13 and $7087 = 19 \times 373$.
Again, we see that $92131 = 13 \times 19 \times 373$.

78.

a)

t	$2t + 1$	$s^2 = t^2 - N$	$s \in \mathbb{Z}$?
157	315	152	$\times$
158	317	467	$\times$
159	319	784	✓

so $t = 159$ and $s = \sqrt{784} = 28$, and $a = s + t = 187$ and $b = t - s = 131$.
Therefore, $24497 = N = ab = 131 \times 187$.

b) Write $N = 131 = 2^s t + 1$ with $s = 1$ and $t = 65$. Since $a^{2^r} t = a^t \equiv -1 \pmod{131}$ for $r = 0$, $n = 131$ is a strong pseudo-prime base 2 and therefore quite likely to be a prime.

c) Note that $2^{40} \equiv 1 \pmod{187}$, so $187|(2^{40} - 1) = (2^{20} - 1)(2^{20} + 1)$.
Calculating $\gcd(187, 2^{20} - 1) = 11$ and $\gcd(n, 2^{20} + 1) = 17$ to find the factors 11 and 17; these are prime and are thus the factors of 187.

79. A very simple method could just be to test the p smallest primes $2, 3, 5, \ldots, p$, to see whether $\frac{n}{2^p - 1}$ is an (odd) integer, and if so, whether it is of the form $2^q - 1$ for some prime q.
For $n = 16646017$, we find that $p = 17$:

$$\frac{n}{2^{17} - 1} = 127 = 2^7 - 1$$

Here, $q = 7$ is prime, and so $n = (2^{17} - 1)(2^7 - 1) = 131071 \times 127$.

80.

a. 0,1,0,1,1

b. As soon as any consecutive 3 bits x_i, x_{i+1}, x_{i+1} reappear later in the list, the output will repeat itself. The numbers $x_0, \ldots, x_9$ are as follows:

$$x_0 = 1, 1, 0, 0, 1, 0, 1, (x_7 =) 1, 1, 0$$

We see that the first sequence 1,1,0 reappears 7 steps later; 7 is therefore the period of this LSFR.

81.

a. The output numbers $x_0, \ldots, x_{19}$ are as follows:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
x_i	1	8	3	4	11	6	7	14	9	10	17	12	13	2	15	16	5	0	1	8

As soon as any number reappears later in the list, the output will repeat itself. We see that $x_0 = 1$ reappears as $x_{18} = 1$; the period of this LSFR is therefore 18.

b. The output numbers $x_0, \ldots, x_{19}$ are as follows:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
x_i	1	0	0	0	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0	1

As soon as any consecutive 3 bits $x_i, \ldots, x_{i+4}$ reappear later in the list, the output will repeat itself. We see that the first sequence 1,0,0,0 reappears 15 steps later; 15 is therefore the period of this LSFR.

82.

a. First, write the message as it has been received:

```
FSOTU
OHFOI
UIJNP
RPUTM
TELHE
HQYEN
```

You can use a number of easy heuristic arguments (for instance, "fourth" goes with "of July", as do "q" and "u") to permute the columns above in the right way but will get the following correct answer:

```
SUTFO
HIOOF
IPNUJ
PMTRU
EEHTL
QNEHY
```

This gives us the message "SHIP EQUIPMENT ON THE FOURTH OF JULY".

b. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}$

c. First, write the message as it has been received:

```
SLAFK
EOROE
LIERO
LLSEV
ASBTE
LHEAR
```

Now permute the columns:

```
LKFSA
OEOER
IORLE
LVELS
SETAB
HRALE
```

The enciphered message is then "LKFSA OEOER IORLE LVELS SETAB HRALE".

83. Looking at the first block HSTII, we might guess that it was enciphered from "THIS I", using one of the permutations

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \qquad \text{and} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$$

Applying the inverse σ_1^{-1} of the first permutation to the 1st three blocks, we get "THIS IS A TON HERAR". This does not seem to make sense, so lets try the inverse $\sigma_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$ of the second permutation: We now get a much more lucid message: `THIS IS ANOTHER ARTICLE ON SECRET CODES PQ`