Solutions to MATH3411 Problems 68–75

68. Both polynomials of degree 1, x and $x+1$, are obviously irreducible, and they are also primitive since there is only a single unit in the fields that they generate.
By the Factor Theorem, all polynomials of degree 2 or 3 are irreducible precisely when they have no root:

$$x^2+x+1\,,\quad x^3+x+1\,,\quad x^3+x^2+1\,.$$

The number of units of $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is $2^2-1=3$ which is prime.
Similarly, there are $2^3-1=7$ (also prime) units of the fields generated by the two 3rd degree polynomials.
By Lagrange's Theorem, the root of each polynomial, and thus each polynomial, is primitive in its generated binary field. In case this is cheating a bit, given that MATH3411 has not introduced us to Lagrange's Theorem, we can check this directly, by finding the order of each root.
For $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle,\ \alpha^2=\alpha+1$:

i	1	2	3	4	5	6	7
α^i	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1	1

We see that α and thus x^2+x+1 is primitive in its generated binary field..
For $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle,\ \alpha^2=\alpha+1$:

i	1	2	3	4	5	6	7
α^i	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1	1

We see that α and thus x^3+x+1 is primitive in its generated binary field..
For $\mathbb{Z}_2[x]/\langle x^3+x^2+1\rangle,\ \alpha^3=\alpha^2+1$:

i	1	2	3	4	5	6	7
α^i	α	α^2	α^2+1	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$	1

We see that α and thus x^3+x^2+1 is primitive in its generated binary field.
When finding the polynomials of degree 4 that are irreducible, we can disregard the ones with roots, leaving

$$x^4+x+1\,,\quad x^4+x^2+1\,,\quad x^4+x^3+1\,,\quad x^4+x^3+x^2+x+1\,.$$

To find whether some of these are reducible, consider the binary monic products of quadratic polynomials, with constant term equal to 1:

$$(x^2+ax+1)(x^2+bx+1)=x^4+(a+c)x^3+acx^2+(a+c)x+1\,.$$

Considering the four (and by symmetry, only three) cases $a,c=0,1$, we find x^4+x^2+1 among our four polynomials above. Removing it from our list give us the three irreducible binary polynomials of degree 4:

$$x^4+x+1\,,\quad x^4+x^3+1\,,\quad x^4+x^3+x^2+x+1\,.$$

In Problem 67, we showed that $x^4 + x + 1$ is primitive in its generated binary field, and in Problem 66, we showed that $x^4 + x^3 + x^2 + x + 1$ is not primitive in its generated binary field.
Let us now consider $x^4 + x^3 + 1$; here, we have that $\alpha^4 = \alpha^3 + 1$.

$\alpha^0 = 1$	$\alpha^8 = \alpha^3 + \alpha^2 + \alpha$
$\alpha^1 = \alpha$	$\alpha^9 = \alpha^2 + 1$
$\alpha^2 = \alpha^2$	$\alpha^{10} = \alpha^3 + \alpha$
$\alpha^3 = \alpha^3$	$\alpha^{11} = \alpha^3 + \alpha^2 + 1$
$\alpha^4 = \alpha^3 + 1$	$\alpha^{12} = \alpha + 1$
$\alpha^5 = \alpha^3 + \alpha + 1$	$\alpha^{13} = \alpha^2 + \alpha$
$\alpha^6 = \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha^{14} = \alpha^3 + \alpha^2$
$\alpha^7 = \alpha^2 + \alpha + 1$	$\alpha^{15} = 1$

We see that $x^4 + x^3 + 1$ is primitive in its generated binary field,

69. Now, $\phi(341) = \phi(11 \times 31) = \phi(11)\phi(31) = 10 \times 30 = 300$, so by Euler's Theorem, $2^{300} \equiv 1 \pmod{341}$. This is not very useful, so consider the powers of 2 modulo 341, to find one that is closer to 0 modulo 341:

$$2^8 = 256 = -85 \qquad 2^9 = -170 \qquad 2^{10} = -340 = 1 \qquad (\text{all in } \mathbb{Z}_{341})$$

Then $2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{341}$, and since $\gcd(2, 341) = 1$, 341 is quasi-prime in base 2.
In contrast, we can calculate that $3^{340} \equiv 56 \not\equiv 1 \pmod{341}$, so 341 is not quasi-prime in base 3.

70.

(a) Now, $561 = 3 \times 11 \times 17$ and $\phi(3) = 2$, $\phi(11) = 10$, and $\phi(17) = 16$, so by Euler's Theorem (or Fermat's Little Theorem) for all integers a coprime to 3, 11, and 17,

$$\begin{aligned} a^{560} &\equiv (a^2)^{280} \equiv 1^{280} \equiv 1 \pmod{3} \\ a^{560} &\equiv (a^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{11} \\ a^{560} &\equiv (a^{16})^{40} \equiv 1^{40} \equiv 1 \pmod{17} \end{aligned}$$

(b) Let a be coprime to 561 and apply the Chinese Remainder Theorem to the above three congruences:

$$a^{560} \equiv 1 \pmod{561}$$

We see that 561 is a Carmichael number.
(A slight variant to using the Chinese Remainder Theorem directly is to note that $a^{560} - 1 = 3m_1 = 11m_2 = 17m_3$ for some integers m_1, m_2, m_3. Since 3, 11, and 17 are prime, each m_i must be a divisible by all three numbers 3, 11, and 17, and thus by their product 561, so $a^{560} - 1 \equiv 0 \pmod{561}$.)

71.
Trying to use the values $a = 2, 3$ with Lucas' Test to prove that 97 is prime fail;
however the value $a = 5$ works: $\gcd(5, 97) = 1$ and, given that the prime factors of 96 are 2 and 3,

$$\begin{aligned} 5^{\frac{96}{3}} &\equiv 5^{32} \equiv 35 \not\equiv 1 \pmod{97} \\ 5^{\frac{96}{2}} &\equiv 5^{48} \equiv -1 \not\equiv 1 \pmod{97} \\ 5^{96} &\equiv 1 \pmod{97} \end{aligned}$$

72.
First note that $N = b^{n-1} + \cdots + b + 1$. Let $d = \gcd(b, N)$. Since $d|b$ and $d|N$, $d|N - (b^{n-1} + \cdots + b) = 1$; hence, $\gcd(b, N) = d = 1$.
Now, since $b^{n-1} \equiv 1 \pmod{n}$, it follows that $b^n \equiv b \pmod{n}$, so $N(b-1) \equiv b^n - 1 \equiv b - 1 \pmod{n}$. Since $\gcd(b-1, n) = 1$, we see that $N \equiv 1 \pmod{n}$, so $N - 1 = sn$ for some integer s. Now, $b^n = N(b-1) + 1 \equiv 1 \pmod{N}$, so

$$b^{N-1} = b^{sn} = (b^n)^s \equiv 1^s \equiv 1 \pmod{N}.$$

We have proved that N is a pseudo-prime base b.
Let n_0 be a pseudo-prime base 2 (for instance any prime) and define the numbers $n_1, n_2, \ldots$ iteratively by $n_i = \frac{2^{n_{i-1}}-1}{2-1} = 2^{n_{i-1}} - 1$. Since n_i is odd, $\gcd(2, n) = 1$, and since $\gcd(2-1, n) = \gcd(1, n) = 1$, it follows by the first part of this question and induction that n_i is a pseudo-prime base 2 for all i, so there are infinitely many pseudo-primes base 2.
Now let n_0 be an odd pseudo-prime base 3 (for instance any prime) and define the numbers $n_1, n_2, \ldots$ iteratively by $n_i = \frac{3^{n_{i-1}}-1}{3-1} = \frac{1}{2}(3^{n_{i-1}} - 1)$. Since $n_i = 3^{n_{i-1}-1} + \cdots + 3 + 1 \equiv 1 \pmod{3}$, we see that $\gcd(3, n_i) = 1$. Furthermore, note that $n_1 \equiv 3^{n_{i-1}-1} + \cdots + 3 + 1 \equiv n_{i-1} \pmod{2}$. Since n_0 is odd, induction gives us that n_{i-1} is also odd for all i. Therefore $\gcd(3-1, n_i) = \gcd(2, n_i) = 1$ for all i. It follows by the first part of this question and induction that n_i is a pseudo-prime base 3 for all i, so there are infinitely many pseudo-primes base 3.
In fact, we can generalise the $b = 2, 3$ to arbitrary values of b; can you see how?

73.
Write $561 = 2^s t + 1$ where $s = 4$ and $t = 35$. Then $2^t = 2^{35} \equiv 263 \not\equiv 1 \pmod{561}$ and

$$\begin{aligned}
r = 0 &: \quad 2^{2^r t} = 2^{35} \equiv 263 \not\equiv -1 \pmod{561} \\
r = 1 &: \quad 2^{2^r t} = 2^{70} \equiv 166 \not\equiv -1 \pmod{561} \\
r = 2 &: \quad 2^{2^r t} = 2^{140} \equiv 67 \not\equiv -1 \pmod{561} \\
r = 3 &: \quad 2^{2^r t} = 2^{280} \equiv 1 \not\equiv -1 \pmod{561}
\end{aligned}$$

so 561 is not a strong pseudo-prime base 2.

74.
Define events

$$\begin{aligned}
C &= \{n \text{ is composite}\} \\
T_k &= \{n \text{ passes } k \text{ Miller-Rabin tests}\}
\end{aligned}$$

We are told to assume that $P(T_k|C) < 4^{-k}$.
Also, since a prime always passes the Miller-Rabin test, $P(T_k|C^c) = 1$. Therefore,

$$\begin{aligned}
P(n \text{ is composite} \mid n \text{ passes } k \text{ Miller-Rabin tests}) = P(C|T_k) &= \frac{P(C \cap T_k)}{P(T_k)} \\
&= \frac{P(T_k|C)P(C)}{P(T_k)} \\
&< 4^{-k} \frac{P(C)}{P(T_k|C)P(C) + P(T_k|C^c)P(C^c)} \\
&= 4^{-k} \frac{P(C)}{P(T_k|C)P(C) + P(C^c)}
\end{aligned}$$

Now, as k grows large, $P(T_k|C)$ tends towards 0, being bounded above by 4^{-k}, so for large k, we have approximately that

$$P(n \text{ is composite} \mid n \text{ passes } k \text{ Miller-Rabin tests}) < 4^{-k}\frac{P(C)}{P(C^c)} = 4^{-k}\frac{P(n \text{ is composite})}{P(n \text{ is prime})}$$

75.
For $n = 14647$, $\lceil\sqrt{n}\rceil = 122$, so

t	$2t+1$	$s^2 = t^2 - n$	$s \in \mathbb{Z}$?
122	245	237	×
123	247	482	×
124	249	729	✓

so $t = 124$ and $s = \sqrt{729} = 27$, and $a = s + t = 151$ and $b = t - s = 97$; hence, $14647 = n = ab = 151 \times 97$.
For $n = 83411$, $\lceil\sqrt{n}\rceil = 289$, so

t	$2t+1$	$s^2 = t^2 - n$	$s \in \mathbb{Z}$?
289	579	110	×
290	581	689	×
291	583	1270	×
292	585	1853	×
293	587	2438	×
294	589	3025	✓

so $t = 294$ and $s = \sqrt{3025} = 55$, and $a = s+t = 349$ and $b = t-s = 239$; hence, $83411 = n = ab = 349\times 239$.
For $n = 200819$, $\lceil\sqrt{n}\rceil = 122$, so

t	$2t+1$	$s^2 = t^2 - n$	$s \in \mathbb{Z}$?
449	899	782	×
450	901	1681	✓

so $t = 450$ and $s = \sqrt{1681} = 409$, and $a = s + t = 491$ and $b = t - s = 409$;
hence, $200819 = n = ab = 491 \times 409$.