Solutions to Practice exam

2 marks 3 marks	1. $x \equiv y \bmod n \quad \Leftrightarrow \quad n \mid (x-y)$. Clearly, multiplying by m, $x \equiv y \bmod n \quad \Rightarrow mx \equiv my \bmod n$ If $gcd(n,m) = 1$ then there are integers a and b such that $an + bm = 1$. Then $bm \equiv 1 \bmod n$. So if $mx \equiv my \bmod n$ then $bmx \equiv bmy \bmod n$, that is, $x \equiv y \bmod n$.
2 marks	a) $3x \equiv 6 \bmod 9 \Leftrightarrow x \equiv 2 \bmod 3$
2 marks	b) $3x \equiv 5 \bmod 6 \Rightarrow 5 \equiv 0 \bmod 3$, which is not true. So there are no integer solutions
2 marks	c) If $x = 0$, 1, 2, 3 or 4, then x^2+x+1 is 1, 3, 2, 1 or 4 $\bmod 5$. So there are no integer solutions. Another more sophisiticated way to do this is to note that, multiplying by $x-1$, $$x^2+x+1 \equiv 0 \bmod 5 \Rightarrow x^3 - 1 \equiv 0 \bmod 5 \Rightarrow x \equiv 1 \bmod 5$$ where the last implication uses Fermat's Little Theorem, and the fact that $gcd(3,4) = 1$. But $1^2 + 1 + 1 \neq 0 \mod 5$ so there are no solutions to the original equation
2 marks	d) $$x^2 \equiv 1 \bmod 7 \Rightarrow (x-1)(x+1) \equiv 0 \bmod 7 \Rightarrow x \equiv \pm 1 \bmod 7.$$
7 marks	e) We have $3^{-1} \equiv 5 \bmod 7$ and $3^{-1} \equiv 2 \bmod 5$. So multiplying the first equation by 5 and the third by 2, our system of simulataneous equations becomes $$x \equiv 5 \bmod 7, \quad x \equiv 5 \mod 6, \quad x \equiv 4 \bmod 5.$$ There is a solution since any two of 5, 6 and 7 are coprime. The lcm of these three is 210 so the answer will be unique $\mod 210$. From the first equation we obtain $x = 5 + 7y$. Substituting in the second equation gives $y \equiv 0 \mod 6$ and hence $y = 6z$ and $x = 42z + 5$. Substituting in the third equation gives $2z + 5 \equiv 4 \bmod 5$, that is, $z \equiv 2 \bmod 5$. So $x \equiv 89 \bmod 210$. Alternatively we can use the Chinese Remainder formula. Since $6 \times 5 = 30 \equiv 2 \mod 7$ has inverse $4 \bmod 7$, $7 \times 5 = 35$ has inverse $5 \bmod 7$ and $7 \times 6 = 42$ has inverse $3 \bmod 5$, the solution is $$x \equiv 5 \times 4 \times 30 + 5 \times 5 \times 35 + 4 \times 3 \times 42 \equiv -30 + 35 + 84 \equiv 89 \bmod 210.$$

4 marks	2a) Since $k \mid n!$ for all $2 \leq k \leq n$, we also have $k \mid n! + k$ for $2 \leq k \leq n$. Since $k+n! > k$, the number $n!+k$ is composite. There are $n-1$ of these numbers and so if p is the largest prime $len! + 1$ and q is the smallest $\geq n!+n+1$ we have $q-p \geq n$, and $G(p,q)$ is a prime gap of length $\geq n$
1 mark	The first 4 primes are: $$2,\ 3,\ 5,\ 7,\ 11.$$ So if we take $p = 7$ then p is the smallest prime such that $G(p,q)$ is a prime gap of length 6 for some q: with $q = 11$ and $G(p,q) = G(7,11)$.
2 marks	b) FTA: Let $n \in \mathbb{Z}_+$ with $n \geq 2$. Then there are primes q_i for $1 \leq i \leq m$ and $q_i < q_{i+1}$ and $k_i \in Z_+$ such that $n = \prod_{i=1}^m q_i^{k_i}$. This representation is unique.
3 marks	Now if $n \in \mathbb{Z}_+$ with $n \geq 2$ is composite, we can write $n = k \times \ell$ for integers k and ℓ with $1 < k \leq \ell < n$. Then $k^2 \leq k \times \ell = n$ and $k \leq \sqrt{n}$. By the FTA there is a prime p with $p \mid k$. But then $p \mid n$ also, and $p \leq \sqrt{n}$ also.
3 marks	We have $7^2 = 49 < 89$ and $11^2 = 121 > 97$. the primes ≤ 7 are 2, 3, 5 and 7. Clearly neither number is divisible by 2 or 5 =– not by 3 since in each case the sum of the digits is not divisible by 3. Also neither number is divisible by 7 as the residues mod 7 of 89 and 97 are 5 and 6 respectively.
1 mark	c)$\pi(x)$ is the number of primes $\leq x$
2 marks	Prime Number Theorem: $$\lim_{x \to +\infty} \frac{\pi(x)}{x/\ln x} = 1.$$
4 marks	If n is sufficiently large given n, we have $\pi(n) \leq \frac{5n}{4 \ln n}$. If m is the largest integer with $p_m \leq n$ then $\pi(n) = m$. If $p_{k+1} - p_k \leq \frac{1}{2} \ln n$ for all $k \leq m$ then $$n \leq p_{m+1} - 1 \leq 1 + \sum_{k=1}^{m} (p_{k+1} - p_k) \leq 1 + \frac{1}{2} \ln n \times m \leq 1 + \frac{1}{2} \times \ln n \times \frac{5}{4} \times \frac{n}{\ln n} = 1 + \frac{5n}{8}.$$ This gives a contradiction if $3n/8 > 1$, in particular, for $n \geq 3$.

2 marks	3. Fermat's Little Theorem: Let p be prime. Then $a^p \equiv a \bmod p$ for all $a \in \mathbb{Z}$, and $a^{p-1} \equiv 1 \bmod p$ if $a \not\equiv 0 \bmod p$.
2 marks	(i) By Fermat's Little Theorem with $p = 17$ we have $a^16 \equiv 1 \bmod 17$ for all integers a which are coprime to 17 – which includes 2 and 3. So, since $96 = 6 \times 16$, $$2^{99} + 3^{98} \equiv 2^3 + 3^2 \equiv 0 \bmod 17,$$ which means that $2^{99} + 3^{98}$ is divisible by 17
4 marks	(ii) The order of any element of G_{17} is a divisor of 16, that is 2^k for any $0 \leq k \leq 4$. We have $2^4 \equiv -1 \bmod 17$ and hence $2^8 \equiv 1$. So 2 has order 8, $4 = 2^2$ has order 4, $4^2 = 16 \equiv -1$ has order 2. Of course, 1 has order 1.To find an element of order 16: $3^2 = 9$ and $3^4 = 81 \equiv -4$. So $3^8 \equiv -1$ and 3 has order 16.
4 marks	The primitive elements are all elements of the form 3^n where n is coprime to 16. There are 8 such elements, given by the odd numbers < 16. Apart from 3 itself we have $3^3 \equiv 10$, $3^5 \equiv 90 \equiv 5$, $3^7 \equiv 45 \equiv 11$, $3^9 \equiv 99 \equiv 14 \equiv -3$, and the others must be $-10 \equiv 7$, $-5 \equiv 12$ and $-11 \equiv 6$. So altogether the primitive elements are $$3,\ 5,\ 6,\ 7,\ 10,\ 11,\ 12,\ 14.$$
3 marks	If $n \equiv 1 \mod 17$ then $$\frac{n^m - 1}{n - 1} = \sum_{k=0}^{m-1} n^k \equiv m \bmod 17,$$ because $n^k \equiv 1 \bmod 17$ for all $k \in \mathbb{N}$. So this is divisible by 17 if and only if m is divisible by 17.
2 marks	If $n \neq 1 \bmod 17$ then $\dfrac{n^m - 1}{n - 1}$ is divisible by 17 if and only if $n^m \equiv 1 \bmod 17$. Since $n \not\equiv 1$, this is only possible if $gcd(m, 16) > 1$, or, equivalently, since $16 = 2^4$, if m is even .
3 marks	If m is even but m is not divisible by 4 and $n^m \equiv 1 \bmod 17$ then $gcd(m, 16) = 2$ and the order of $n \mod 17$ must be 2. The only possibility is $n \equiv -1 \bmod 17$. If m is divisible by 4 but not 8 then $gcd(m, 16) = 4$ and if $n^m \equiv 1 \bmod 17$ then the order of $n \bmod m$ must be 2 or 4. The elements of order 4 are $\pm 4 \bmod 17$. So the only possible solutions are $-1 \bmod 17$ and $\pm 4 \bmod 17$.

<table>
<tr><td>1 mark</td><td>4. For any integer $n \in \mathbb{Z}_+$, $\phi(n)$ is the number of $k \in \mathbb{Z}_+$ with $k \leq n$ such that $gcd(k, n) = 1$</td></tr>
<tr><td>2 marks</td><td>If p is prime and $a \geq 1$, then for $k \leq p^a$, we have

$$gcd(k, p^a) > 1 \Leftrightarrow p \mid k \ \Leftrightarrow k = p\ell, \quad 1 \leq \ell \leq p^{a-1}.$$

So

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1).$$</td></tr>
<tr><td>2 marks</td><td>The divisors of p^a are p^i for $0 \leq i \leq a$, and

$$\int p^a = \sum_{i=0}^{a} p^i = \frac{p^{a+1}-1}{p-1}.$$</td></tr>
<tr><td>3 marks</td><td>If

$$n = \prod_{i=1}^{m} p_i^{k_i}$$

where the p_i are all distinct primes and $m_i \geq 1$ then

$$\phi(n) = \prod_{i=1}^{m} p_i^{k_i-1}(p_i - 1),$$

and

$$\int n = \prod \frac{p_i^{k_i+1}-1}{p_i - 1}.$$</td></tr>
<tr><td>3 marks</td><td>We have

$$2016 = 2^3 \times 252 = 2^5 \times 63 = 2^5 \times 3^2 \times 7.$$

So

$$\phi(2016) = 2^4 \times 3 \times 2 \times 6 = 64 \times 9 = 576.$$</td></tr>
<tr><td>3 marks</td><td>$$\begin{aligned} \phi(11!) &= \phi(2 \times 3 \times 2^2 \times 5 \times 2 \times 3 \times 7 \times 2^3 \times 3^2 \times 2 \times 5 \times 11) \\ &= \phi(2^8 \times 3^4 \times 5^2 \times 7 \times 11) = 2^7 \times 3^3 \times 2 \times 5 \times 2^2 \times 6 \times 10 \\ &= 2^{12} \times 3^4 \times 5^2 = 8294400. \end{aligned}$$</td></tr>
<tr><td>6 marks</td><td>If p is prime and $p \mid n$ then $p - 1 \mid \phi(n)$. If p is an odd prime then $\phi(p^k) = p^{k-1}(p-1)$ is even for any integer $k \geq 1$, and $\phi(2^k) = 2^{k-1}$. Taking the product of these we see that $\phi(n)$ is even for all n, unless $n = 2$, and $\phi(2) = 1$ If $n = n_1 n_2$ then $\phi(n) = \phi(n_1)\phi(n_2)$. If $\phi(n) = 10$ and $n = n_1 n_2$ for coprime n_1 and n_2 then, without loss of generality, $\phi(n_1) = 10$ and $\phi(n_2) = 1$. So $n_2 = 2$ and n_1 is odd – and prime. So $n_1 = 11$. So the only possibilities are $n = 11$ and $n = 22$.</td></tr>
</table>

3 marks	5. If $x \equiv y \bmod n_1$ and $x \equiv y \bmod n_2$ then $n_1 \mid x - y$ and $n_2 \mid x - y$. Since n_1 and n_2 are coprime, this means that $n_1 n_2 \mid x - y$ and hence $x \equiv y \bmod (n_1 n_2)$.
2 marks	For example take $n_1 = 4$ and $n_2 = 6$. Take $x = 12$ and $y = 0$. Then $x \equiv y \bmod 4$ and $x \equiv y \bmod 6$ but $x \not\equiv y \bmod 24$
4 marks	$2046 = 11 \times 186$ and $2^{2046} = (2^{11})^{186} \equiv 1^{186} \equiv 1 \bmod 2047$ If $2^{11} \equiv 1 \bmod p$ then by Fermat's Little Theorem $gcd(11, p-1) > 1$ and hence since 11 is prime we have $11 \mid p - 1$, that is, $p \equiv 1 \bmod 11$. The only primes satisfying this under 100 are 23, 67 and 89. It is easily verified that 23 divides 2047 and $2047 = 23 \times 89$.
2 marks	Korselt's condition on n is that $n = \prod_{i=1}^{m} p_i$ where all the p_i are distinct primes, and $p_i - 1 \mid n - 1$ for all i.
3 marks	$2821 = 7 \times 403 = 7 \times 13 \times 31$ s a product of distinct primes, and $2820 = 2^2 \times 705 = 2^2 \times 5 \times 141 = 2^2 \times 5 \times 3 \times 47$. Since $7 - 1 = 2 \times 3$ and $13 - 1 = 2^2 \times 3$ and $30 - 2 \times 3 \times 5$ all of these divide 2820, and 2821 is a Carmichael number.
1 mark	If $a^{n-1} = b^{n-1} \equiv 1 \bmod n$ then $(ab^{-1})^{n-1} \equiv 1 \bmod n$. So the set of pseudoprimes is a group
5 marks	As above, we have $G_{35} \cong G_5 \times G_7$. Since 5 and 7 are prime, the groups G_5 and G_7 are cyclic of orders $4 = 5 - 1$ and $6 = 7 - 1$. So the order of any element of G_{35} is a divisor of $lcm(6, 4) = 12$. Now $34 = 2 \times 17$. For $a \in G_{35}$, 35 is a pseudoprime to base a (or $a \equiv 1$) if and only if $a^{34} \equiv 1 \bmod 35$. Since $gcd(12, 34) = 2$ this happens if and only if $a^2 \equiv 1 \bmod 35$. Since $a^2 \equiv 1 \bmod 5$ for just two elements of G_5, and $a^2 \equiv 1 \bmod 7$ for just two elements of G_7 there are four such elements of G_{35}. They clearly include $\pm 1 \bmod 35$. The others are $\pm 6 \bmod 35$.

3 marks	6a) For any $z \in \mathbb{C}$, write $z = x + iy$ for real x and y. then there are integers q_1 and q_2 such that $\|x - q_1\| \le \frac{1}{2}$ and $\|y - q_2\| \le \frac{1}{2}$. Then if $q = q_1 + iq_2$ we have $q \in \mathbb{Z}[i]$ and $\|z - q\|^2 \le \frac{1}{4} + \frac{1}{4} \le \frac{1}{2}$. Now let a and $b \in \mathbb{Z}[i]$ with $b \neq 0$ and let $q \in \mathbb{Z}[i]$ with $\|a/b - q\|^2 \le \frac{1}{2} < 1$. Then write $r = a - qb \in \mathbb{Z}[i]$. We have $v(r)\|r\|^2 = \|z - q\|^2\|b\|^2 < \|b\|^2 = v(b)$ and $a = qb + r$. Also $v(cd) = \|c\|^2\|d\|^2 \ge \|c\|^2 = v(c)$ for all c and $d \in \mathbb{Z}[i]$ with $d \neq 0$. So both properties of a Euclidean function hold.
3 marks	b) Since conjugation is multiplicative, $$n = (s + it)(u + iv) \ \Leftrightarrow \ n = (s - it)(u - iv).$$ So $s + it$ divides n if and only if $s - it$ does, and $$s + it \mid n \Rightarrow s^2 + t^2 \mid n^2.$$
3 marks	If $$n_j = s_j^2 + t_j^2 = (s_j + it_j)\overline{s_j + it_j}$$ then $$n_1n_2 = (s_1+it_1)(s_2+it_2)\overline{(s_1 + it_1)(s_2 + it_2)} = (s_1s_2-t_1t_2)^2+(s_1t_2+s_2t_1)^2.$$
3 marks	c) Since $s + it$ is prime in $\mathbb{Z}[i]$, we have $gcd(s, t) = 1$. If $$(s + it)(s - it)s^2 + t^2 = uv$$ for integers u and $v \ge 2$, then neither u nor v divides $s + it$ in $\mathbb{Z}[i]$, contradicting unique factorisation. So $s^2 + t^2$ must be prime, and since $s^2 + t^2 \mid n^2$ by a), we have $s^2 + t^2 \mid n$.
5 marks	d) If $n = s^2 + t^2$ then we can write $$s + it = d\prod_{j=1}^{k}(s_j + it_j)$$ where $d \in \mathbb{Z}$ and s_j and t_j are both non-zero integers, for all $1 \le j \le k$, and $s_j + it_j$ is prime in $\mathbb{Z}[i]$. This gives $$s^2 + t^2 = d^2\prod_{j=1}^{k}(s_j^2 + t_j^2)$$ and by d) $s_j^2 + t_j^2$ is a positive prime integer for each $1 \le j \le k$. We have $k \ge 1$ because both s and t are non-zero .
3 marks	e) Suppose there are only finitely many such primes q_j for $1 \le j \le n$, and let $N_1 = \prod_{j=1}^{n} q_j^2$ and $N = N_1^2 + 1$. Then $N = N_1^2 + 1^2$ is a sum of two non-zero integer squares. By d) there is a prime integer p dividing N which is also a sum of two integer squares. But then $p = q_j$ for some j. This is impossible because q_j divides N_1 and cannot also divide $N = N_1^2 + 1$.

2 marks	7. The Legendre symbol is defined by $$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } q \equiv a^2 \bmod p \text{ for some } a \in \mathbb{Z} \\ -1 & \text{otherwise} \end{cases}$$
5 marks	If $q \equiv a^2 \mod p$ then$q^{(p-1)/2} \equiv a^{p-1} \equiv 1$ by Fermat's Little Theorem. Conversely if $q^{(p-1)/2} \equiv 1$ and b is a primitive element of G_p and $q = b^m$ then $b^{m(p-1)/2} \equiv 1$ implies that $p - 1 \mid m(p-1)/2$, that is, m must be even and hence $q \equiv (b^{(m-1)/2})^2$. Since $$F(q_1q_2) \equiv (q_1q_2)^{(p-1)/2} \equiv q_1^{(p-1)/2}q_2^{(p-1)/2} \equiv F(q_1)F(q_2) \bmod p$$ we see that $q \mapsto F(q) \bmod p$ is a homomorphism. Since $-1 \not\equiv 1 \bmod p$ we see that F itself is a homomorphism.
2 marks	$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$
3 marks	For any odd prime p, $$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p = \pm 1 \mod 8.$$ If p and q are odd primes, then $$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}.$$
2 marks	So $\left(\frac{2}{p}\right)$ and $\left(\frac{-1}{p}\right)$ have the same sign if and only if $p = 1 \bmod 8$ — when they are both 1 – or $p \equiv 3 \bmod 8$ — when they are both -1.
2 marks	$$\left(\frac{5}{19}\right) \times \left(\frac{19}{5}\right) = (-1)^{2\times 9} = 1 \text{ and } \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1$$ since $4 = 2^2$. So $$\left(\frac{5}{19}\right) = 1.$$

4 marks	We have $$\left(\frac{46}{89}\right) = \left(\frac{23}{89}\right) \times \left(\frac{2}{89}\right) = 1 \times \left(\frac{23}{89}\right)$$ since $89 \equiv 1 \mod 8$.Then $$\left(\frac{23}{89}\right) \times \left(\frac{89}{23}\right) = (-1)^{11\times 44} = 1.$$ Then $$\left(\frac{89}{23}\right) = \left(\frac{20}{23}\right) = \left(\frac{2}{23}\right)^2 \times \left(\frac{5}{23}\right) = \left(\frac{5}{23}\right)$$ and $$\left(\frac{5}{23}\right) \times \left(\frac{23}{5}\right) = (-1)^{2\times 11} = 1.$$ Then $$\left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1.$$ So altogether we have $$\left(\frac{46}{89}\right) = \left(\frac{3}{5}\right) = -1.$$