1. In each part of this problem, full marks will be given if the correct answer is written in the box. If your answer is incorrect, your work will be assessed for part marks.

**[3]** (a) Convert $(4321)_6$ to base 10.

$$4 \times 6^3 + 3 \times 6^2 + 2 \times 6^1 + 1 \times 6^0$$

$$= 4 \times 216 + 3 \times 36 + 2 \times 6 + 1 \times 1$$

$$= 864 + 108 + 12 + 1$$

$$= 985.$$

985

[3] (b) Convert $(2345)_{10}$ to base 16, using A, B, C, D, E, F to represent the digits for 10, 11, 12, 13, 14 and 15 respectively.

$2345 = 146 \times 16 + 9$

$146 = 9 \times 16 + 2$

$9 = 0 \times 19 + 9$

So $(2345)_{10} = (929)_{16}$.

929

[3] (c) Calculate $\text{lcm}(2^5 3^2 5^4 7, 960960)$.

$960960 = 2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

$\text{lcm}(2^5 3^2 5^4 7, 960960) = 2^6 \cdot 3^2 \cdot 5^4 \cdot 7 \cdot 11 \cdot 13$

using theorem 2.58

$2^6 \cdot 3^2 \cdot 5^4 \cdot 7 \cdot 11 \cdot 13$.

[3] (d) Determine the digit $d$ so that $(2d4\ 000\ 000\ 234\ 458)_{10}$ is divisible by 9.

Sum of digits $= 2+d+4+2+3+4+4+5+8$

$= 32+d.$

a number is divisible by 9 $\Leftrightarrow$ the sum of its digits is divisible by 9.

(Thm 3.21).

So we need $9 \mid 32+d$ and $0 \leq d \leq 9$.

It follows (by inspection) that $d=4$.

$\boxed{d=4}$

[3] (e) Determine the remainder when $3^{302} - 5^{200}13^{88}$ is divided by 13.

$3^{302} = (3^3)^{100} \cdot 3^2$

But $3^3 = 27 \equiv 1 \pmod{13}$

So $3^{302} \equiv 9 \pmod{13}$.

And $5^{200}13^{88} \equiv 0 \pmod{13}$

So the remainder is 9.

9

[3] (f) Determine $[3]^{-1}$ in $\mathbb{Z}_{41}$

Want to find $x \in \mathbb{Z}_{41}$ s.t.

$[3][x] = [1]$.

i.e. $3x \equiv 1 \pmod{41}$.

Using EEA to find a solution to

$3x + 41y = 1$.

| | | | |
|---|---|---|---|
| 0 | 1 | 41 | |
| 1 | 0 | 3 | |
| -13 | 1 | 2 | 13 |
| (14) | -1 | 1 | 1 |
| -41 | 3 | 0 | 2 |

14

So $[3]^{-1} = [14]$ in $\mathbb{Z}_{41}$.

[5] 2. Prove that every integer greater than 1 can be expressed as a product of primes.

Suppose for a contradiction that there exists an integer (1) that cannot be written as a product of primes.

Let $N$ be the smallest such integer.

(2) By assumption, $N$ is not prime.

Hence $N$ is composite so

(3) $N = r \cdot s$ for some $r, s \in \mathbb{Z}$ where $1 < r \leq s < N$.

But $N$ is the smallest integer not a product of primes, so $r$ and $s$ can be written as a product of primes.

(4) Hence $r \cdot s$ is a product of primes.

(5) Thus every integer greater than 1 can be written as a product of primes.

[5] 3 Let $a, b, c$ be integers. Prove that if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

If $a \equiv b \pmod{m}$,
then $m \mid (a-b)$. (1)

If $b \equiv c \pmod{m}$
then $m \mid (b-c)$. (2)

Hence $m \mid (a-b) + (b-c)$ (3)

$\iff m \mid (a-b+b-c)$

$\iff m \mid (a-c)$ (4)

Thus $a \equiv c \pmod{m}$. (5)

[8] 4. Solve the simultaneous congruences

① $x \equiv 8 \pmod{27}$

② $x \equiv 2 \pmod{25}$

From ①, $x = 8 + 27y \quad y \in \mathbb{Z}$ [1]

Substitute into ②: $8 + 27y \equiv 2 \pmod{25}$ [+1]

$2y \equiv -6 \pmod{25}$

$y \equiv -3 \pmod{25}$

$y \equiv 22 \pmod{25}$

$\therefore \quad y = 22 + 25z, \; z \in \mathbb{Z}$ [+2]

$\therefore \quad x = 8 + 27(22 + 25z), \; z \in \mathbb{Z}$ [+1]

$= 8 + 594 + 675z$

$= 602 + 675z, \; z \in \mathbb{Z}$ [+2]

$\therefore \quad x \equiv 602 \pmod{675}$ [+1]

[4] 5. If $\gcd(m, n) = d$, when do the simultaneous congruences

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n}$$

have a solution?

Any solution to $x \equiv a \pmod{m}$

(1) is of the form $x = ym + a$, $y \in \mathbb{Z}$.

Substituting into the second equation yields

(2) $ym + a \equiv b \pmod{n}$

$\iff ym \equiv b - a \pmod{n}$

(3) $\iff my \equiv b - a \pmod{n}$

This equation has a soln if and only if

$$\gcd(m,n) \mid (b-a)$$

(4) by Theorem 3.54.

In other words, a solution exists if

$$d \mid (b-a).$$

[5] 6. If $p$ is prime and $k$ is the smallest positive integer such that $a^k \equiv 1 \pmod{p}$ then prove that $k$ divides $p-1$.

Since $a^k \equiv 1$, $a \neq 0$, $p \nmid a$ [1]

$\therefore$ $a^{p-1} \equiv 1 \pmod{p}$, Fermat's Little Thm [+1]

Note: Just Because $a^k \equiv 1 \equiv a^{p-1} \pmod{p}$

it does not follow that $k = p-1$

for example $1^k \equiv 1$ for all $k$!!!

Suppose $k \nmid (p-1)$

Then $\exists\, q, r$, $0 < r < k$

$\ni$ $(p-1) = qk + r$ (Division Algorithm)

$$a^{p-1} \equiv a^{qk+r} \equiv (a^k)^q a^r \equiv 1 \pmod{p}$$ [+2]

But $a^k \equiv 1$ $\therefore$ $a^r \equiv 1$

But $r < k$ which contradicts the fact that $k$ is the smallest positive integer such that $a^k \equiv 1 \pmod{p}$

$\therefore$ $k \mid (p-1)$ [+1]

This page is intentionally blank for rough work.

#6 continued.

Recall mod 7

| $a^1$ | 0 | (1) | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a^2$ | 0 | 1 | 4 | 2 | 2 | 4 | 1 |
| $a^3$ | 0 | 1 | (1) | 6 | 1 | 6 | 6 |
| $a^4$ | 0 | 1 | 2 | 4 | 4 | 2 | 1 |
| $a^5$ | 0 | 1 | 4 | 5 | 2 | 3 | 6 |
| $a^6$ | 0 | 1 | 1 | (1) | 1 | 1 | 1 |
| $a^7$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| $k$ | — | 1 | 3 | 6 | 3 | 6 | 2 |

For mod 7, when $a \equiv 1$, $k = 1$;

when $a \equiv 2, 4$, $k = 3$;

when $a \equiv 3, 5$, $k = 6$;

when $a \equiv 6$, $k = 2$;

in each case $k \mid 6 = p - 1$.