MATH 312 ASSIGNMENT 5 MARK SCHEME 23 Nov '12

Each of the 20 questions is worth 5 marks.

---

① $12345 \equiv 25 \pmod{28}$

$-54321 \equiv 27 \pmod{28}$

---

② $1! + 2! + 3! + \cdots + 100! \pmod{12}$

$\equiv 1! + 2! + 3! + 0 + 0 + \cdots + 0 \pmod{12}$

{since $n!$ for $n \geq 4$ contains $12 = 2^2 \cdot 3$ as a factor}

$\equiv 1 + 2 + 6 \equiv 9 \pmod{12}$

$1! + 2! + 3! + \cdots + 100! \pmod{25}$

$\equiv 1! + 2! + \cdots + 9! + 0 + 0 + \cdots + 0 \pmod{25}$

{since $n!$ for $n \geq 10$ contains $25 = 5^2$ as a factor}

$\equiv 1 + 2 + 6 + 24 + 20 + 20 + 15 + 20 + 5$

$\equiv 113 \equiv 13 \pmod{25}$

---

(3) Let $d_1 := \gcd(a, c)$ $\quad d_1 \in \mathbb{N}$

Let $d_2 := \gcd(b, c)$ $\quad d_2 \in \mathbb{N}$

$a \equiv b \pmod{c} \iff a + cs = b$ for some $s \in \mathbb{Z}$.

Since $d_1 \mid a$ and $d_1 \mid c$, $d_1 \mid b = a + cs$.

But also $d_1 \mid c \Rightarrow d_1 \mid \gcd(b, c) = d_2$.

Since $d_2 \mid b$ and $d_2 \mid c$, $d_2 \mid a = b - cs$.

But also $d_2 \mid c \Rightarrow d_2 \mid \gcd(a, c) = d_1$

$$\left.\begin{array}{l} d_1 \mid d_2 \\ d_2 \mid d_1 \\ d_1, d_2 \in \mathbb{N} \end{array}\right\} \; d_1 = d_2.$$

---

(4) {By induction on $j \geq 2$}.

We know (from class/textbook) that for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}$,

$$\left.\begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array}\right\} \text{ implies } a_1 a_2 \equiv b_1 b_2 \pmod{m}$$

This is the Base Case and helps our Induction step.

For then

$$\left.\begin{array}{l} a_1 a_2 \cdots a_j \equiv b_1 b_2 \cdots b_j \pmod{m} \\ a_{j+1} \equiv b_{j+1} \pmod{m} \end{array}\right\} \text{ implies } a_1 \cdots a_j \equiv b_1 \cdots b_j \pmod{m}$$

Thus, by induction, $a_1 a_2 \cdots a_m \equiv b_1 b_2 \cdots b_m \pmod{m}$

(5) For $n=1$, $5^n \equiv 5^1 \equiv 1+4(1) \equiv 1+4n \pmod{16}$.

Now suppose $5^k \equiv 1+4k \pmod{16}$ for some $k \in \mathbb{N}$.

Then $5^{k+1} = 5 \cdot 5^k$

$\equiv 5(1+4k) \pmod{16}$

$\equiv 5 + 20k \pmod{16}$

$\equiv 5 + 4k \pmod{16}$

$\equiv 1 + 4k + 4 \pmod{16}$

$\equiv 1 + 4(k+1) \pmod{16}$.

Thus, by induction, $5^n \equiv 1+4n \pmod{16}$ for all $n \in \mathbb{N}$.

---

(6) As 17 is a prime, by Wilson's Theorem, we get

$16! \equiv (17-1)! \equiv -1 \equiv 16 \pmod{17}$.

As 11 is a prime and $\gcd(3, 11) = 1$, by Fermat's Little Theorem, $3^{10} \equiv 1 \pmod{11}$

Alternatively, $310 \equiv 2 \pmod{11}$

(7)

$x \pmod 8$	$y \pmod 8$
1	1, 3, 5 or 7
3	0, 2, 4 or 6
5	1, 3, 5 or 7
7	0, 2, 4 or 6

[Remark: Instead of doing the question directly, we can use the property

$$ax \equiv ay \pmod m \iff x \equiv y \left(\mod \frac{m}{\gcd(a,m)}\right)$$

to reduce the question to

$$x + 2y \equiv 3 \pmod 4.$$

This gives $x \equiv 1 \pmod 4 \Rightarrow y \equiv 1, 3$

$x \equiv 3 \pmod 4 \Rightarrow y \equiv 0, 2$

And then you can recover the solutions above $\pmod 8$.]

(8) Seek to solve

$$x \equiv 2 \pmod 3$$
$$x \equiv 0 \pmod 4$$
$$x \equiv 2 \pmod 5$$

Here's an "algorithmic" version of the book's method which works well for easy integers.

$x \equiv 2 \pmod 3 \Longrightarrow x = 2, 5, \textcircled{8}, 11, \ldots$

$\Downarrow$

$0 \pmod 4$

So by the CRT, $x \equiv 8 \pmod{12}$ $\{\gcd(3,4) = 1\}$

$x = 8, 20, \textcircled{32}, 44, \ldots$

$\Downarrow$

$2 \pmod 5$

So one such integer is 32.

[Of course, by the CRT, any integer x s.t.

$x \equiv 32 \pmod{60}$ would work.

Note: 3, 4, 5 are pairwise coprime]

---

(9) As $5(7) = 35 \equiv 1 \pmod{17}$,

the multiplicative inverse of $5 \pmod{17}$ is 7.

(10) $x \equiv 4 \pmod 6$ → $x \equiv 4 \equiv 0 \pmod 2$

→ $x \equiv 4 \equiv 1 \pmod 3$

$x \equiv 13 \pmod{15}$ → $x \equiv 13 \equiv 1 \pmod 3$

→ $x \equiv 13 \equiv 3 \pmod 5$

So this problem reduces to solving the system of linear congruences

$$\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

But the first two are already solved by $x \equiv 4 \pmod 6$.

$x = 4, 10, 16, 22, 28, 34, \ldots$

$\Downarrow$

$28 \equiv 3 \pmod 5$

So by the CRT, the solution is any x s.t.

$$x \equiv 28 \pmod{30}$$

---

(11) $\exp_5(235,555,790) = 1$

"Highest power of 5 that divides"

$\exp_2(89,375,744) = 10$

(12) $(1+8+3+0+1)-(0+6+2+0+5)$

$= 13 - 13 = 0.$

Since $11 \mid 0$, yes, 1086320015 is divisible by 11.

---

(13) $2340 = 2^2 \cdot 3^2 \cdot 5 \cdot 13.$

So only 13 divides 2340.

---

(14) $x_7 \equiv 7(1) + 3(3) + 1(2) + 7(9) + 3(9) + 1(9) \pmod{10}$

$\equiv 117 \pmod{10}$

$\equiv 7 \pmod{10}$

The check digit is 7.

---

(15) For p prime, by Fermat's Little Theorem,

$$1^{p-1} + 2^{p-1} + \cdots + (p-2)^{p-1} + (p-1)^{p-1}$$

$$\equiv \underbrace{1 + 1 + \cdots + 1 + 1}_{(p-1) \text{ times}} \pmod{p}$$

$$\equiv p - 1 \pmod{p}$$

$$\equiv -1 \pmod{p}.$$

(16) n odd composite integer, pseudoprime base a

$\Downarrow$

$$a^n \equiv a \pmod{n}$$

$\Downarrow$

Note: n odd

$$(n-a)^n = n^n - \binom{n}{1} n^{n-1} a^1 + \cdots - \binom{n}{n-1} n^1 a^{n-1} - a^n$$

Binomial expansion

$$\equiv n^n - a^n \pmod{n}$$

since $n \mid \binom{n}{k}$ for $k = 1, 2, \ldots, n-1$

$$\equiv n - a \pmod{n}$$

since $b^n \equiv b \pmod{n}$ for all $b \in \mathbb{Z}$.

$\Downarrow$

n is a pseudoprime to the base $(n-a)$

(17) $r_1 = 2$ $\quad \gcd(2-1, 7331117) = 1$.

$r_2 = 2^2 \equiv 4 \pmod{7331117}$ $\quad \gcd(4-1, 7331117) = 1$

$r_3 = 4^2 \equiv 16 \pmod{7331117}$ $\quad \gcd(16-1, 7331117) = 1$

$r_4 = 16^2 \equiv 256 \pmod{7331117}$ $\quad \gcd(256-1, 7331117) = 1$

$r_5 = 256^2 \equiv 65536 \pmod{7331117}$ $\quad \gcd(65535, 7331117) = 1$.

$r_6 = 65536^2 \equiv 6263851 \pmod{7331117}$ $\quad \gcd(6263850, 7331117) = 1$.

$r_7 = 6263851^2 \equiv 6404232 \pmod{7331117}$ $\quad \gcd(6404231, 7331117) = 641$

So a divisor of 7331117 is 641

---

(18) $2^{18} = 262144 = 189(1387) + 1 \equiv 1 \pmod{1387}$.

So $2^{1387} = 2^{1386} \cdot 2$

$= (2^{18})^{77} \cdot 2$

$\equiv 1^{77} \cdot 2 \pmod{1387}$

$\equiv 2 \pmod{1387} \implies$ 1387 is a pseudoprime to the base 2.

$1387 - 1 = 1386 = (2^1)(693)$.

But $(2^0)(693) = 693$ and $2^{693} = (2^{18})^{38} \cdot 2^9$

$\equiv 1^{38} \cdot 512 \pmod{1387}$

$\not\equiv \pm 1 \pmod{1387}$

So 1387 does <u>not</u> pass Miller's test for the base 2

$\implies$ 1387 is <u>not</u> a strong pseudoprime to the base 2.

(19) $321197185 = 5 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 137$

For any $b \in \mathbb{Z}$ s.t. $(b, 321197185) = 1$,
we have $(b,5) = (b,19) = (b,23) = (b,29) = (b,37) = (b,137) = 1$

So by applications of Fermat's Little Theorem over the various primes, we get

$$b^{321197184} = (b^4)^{80299296} \equiv 1^{80299296} \equiv 1 \pmod 5$$

$$b^{321197184} = (b^{18})^{17844288} \equiv 1^{17844288} \equiv 1 \pmod{19}$$

$$b^{321197184} = (b^{22})^{14599872} \equiv 1^{14599872} \equiv 1 \pmod{23}$$

$$b^{321197184} = (b^{28})^{11471328} \equiv 1^{11471328} \equiv 1 \pmod{29}$$

$$b^{321197184} = (b^{36})^{8922144} \equiv 1^{8922144} \equiv 1 \pmod{37}$$

$$b^{321197184} = (b^{136})^{2361744} \equiv 1^{2361744} \equiv 1 \pmod{137}$$

And as 5, 19, 23, 29, 37 and 137 are distinct primes, by the CRT, we get

$$b^{321197184} \equiv 1 \pmod{321197185}$$

Since this is true for all $b \in \mathbb{Z}$ s.t. $(b, 321197185) = 1$, $\therefore$ 321197185 is a Carmichael number

(20) Residue classes (mod 14)

a	$\gcd(a, 14)$
0	14
1	1
2	2
3	1
4	2
5	1
6	2
7	7
8	2
9	1
10	2
11	1
12	2
13	1

So a reduced residue system mod 14 is

$\{1, 3, 5, 9, 11, 13\}$.