FINAL EXAM 2002

(p.1)

1. Let $a,b,c \in \mathbb{Z}$ with $(a,b)=1$.

Suppose ~~a|c~~ $a|c$ and $b|c$.

Then $c = ad$ & $c = be$ for some $e,d \in \mathbb{Z}$.

$(a,b)=1$ implies that

$$ax+by=1$$

for some $x,y \in \mathbb{Z}$. So

$$c(ax+by) = c$$

$$acx + cby = c,$$

$$a(be)x + (ad)by = c,$$

$$ab(ex+dy)=c.$$

Therefore $ab|c$ since $ex+dy \in \mathbb{Z}$.

2. Suppose $a,b,c \in \mathbb{Z}$, a and b are not both zero & $d=(a,b)$.

($\Rightarrow$) Suppose $ax+by=c$ for some integers x,y. $d|a$ & $d|b$ & hence $d|ax+by$ & $d|c$.

($\Leftarrow$) Suppose $d|c$. Then $c = de$ for some $e \in \mathbb{Z}$.

By the Hint:

$$d = ma+nb$$

for some $m,n \in \mathbb{Z}$. So

$$c = ed = e(ma+nb) = a(em) + b(en)$$

& $ax+by=c$

where $x=em$, $y=en \in \mathbb{Z}$.

3(i) SEE 2009 EXAM

(ii) Since 2, 73, 1103 are pairwise relatively prime it suffices to show that

(*) $\quad 2^{161038} \equiv 2 \pmod{m}$

for $m = 2$, 73 and 1103.

$2^{161038} \equiv 0 \equiv 2 \pmod{2}$ & (*) holds for $m = 2$.

By Fermat's Little Theorem

$$2^{72} \equiv 1 \pmod{73}$$

since 73 is an odd prime.

$$161038 = (2236)(72) + 46,$$

$$2^{161038} = (2^{72})^{2236}\, 2^{46} \equiv 2^{46} \pmod{73}$$

$$2^6 = 64$$

$$2^7 = 128 \equiv 55 \pmod{73}$$

$$2^8 \equiv 110 \equiv 37 \pmod{73}$$

$$2^9 \equiv 74 \equiv 1 \pmod{73}.$$

Thus

$$2^{46} = (2^9)^5\, 2^1 \equiv 2 \pmod{73}$$

& (*) holds for $m = 73$.

By Fermat's Little Theorem

$$2^{1102} \equiv 1 \pmod{1103}$$

Since 1103 is an odd prime.

$$161038 = (146)(1102) + 146$$

$$2^{161038} = (2^{1102})^{146} \cdot 2^{146} \equiv 2^{146} \pmod{1103}$$

$$2^4 = 16$$
$$2^8 = 16^2 = 256$$
$$2^{16} = 65536 = (59)(1103) + 459 \equiv 459 \pmod{1103}$$
$$2^5 = 32$$
$$2^{13} = 2^5 \cdot 2^8 = (32)(256)$$
$$= \cancel{8426}\ 8192 = 7(1103) + 471$$
$$\equiv 471 \pmod{1103}$$
$$2^{29} = 2^{13} \cdot 2^{16} \equiv (459)(471) \pmod{1103}$$
$$\equiv 216189 \pmod{1103}$$
$$\equiv 1 \pmod{1103}$$

since $216189 = (1103)(196) + 1$.

$$2^{161038} \equiv 2^{145} \cdot 2 \pmod{1103}$$
$$\equiv (2^{29})^5 \cdot 2 \pmod{1103}$$
$$\equiv 2 \pmod{1103} \quad (\text{since } 2^{29} \equiv 1 \pmod{1103})$$

& (*) holds for $m = 1103$.
It follows that 161038 is pseudoprime.

4.

(i) <u>Euler's Theorem</u> Let $a, m \in \mathbb{Z}$, $m > 0$ & suppose $(a, m) = 1$.
Then
$$a^{\phi(m)} \equiv 1 \pmod m$$

(ii) Suppose m, n are positive relatively prime integers.
Then $m^{\phi(n)} \equiv 1 \pmod n$ (by Euler's Thm)
& $n^{\phi(m)} \equiv 0 \pmod n$ (since $\phi(m) \geq 1$),
&
$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 + 0 \equiv 1 \pmod n.$$

Similarly, $n^{\phi(m)} \equiv 1 \pmod m$ (by Euler's Thm), &

$m^{\phi(n)} \equiv 0 \pmod m$ (since $\phi(n) \geq 1$), &

$m^{\phi(n)} + n^{\phi(m)} = 0 + 1 \equiv 1 \pmod m$.

Hence

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod k$$

for $k = m$ & $k = n$. It follows that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$$

since m, n are relatively prime.

5(i) SEE 2009 EXAM

(ii) Suppose f is multiplicative & $f(1) = 0$.
Suppose n is a positive integer. Then
$(n, 1) = 1$ &

$$f(n) = f(n \cdot 1) = f(n) f(1) \quad \text{(since } f \text{ is multiplicative)}$$
$$= f(n) \cdot 0 = 0.$$

So

$$f(n) = 0 \text{ for all } n.$$

(iii) Suppose f is multiplicative & $f(1) \neq 0$.
Then $(1, 1) = 1$ &

$$f(1) = f(1 \cdot 1) = f(1) f(1) \quad \text{since } f \text{ is multiplicative}$$

Since $f(1) \neq 0$

$$\frac{f(1)}{f(1)} = \frac{f(1) f(1)}{f(1)} \quad \& \quad f(1) = 1.$$

(iv) SEE 2009 EXAM

6.

(i) Suppose m, n are positive integers & $m \mid n$.

<u>Case 1</u> $m = 1$. Then $\phi(m) = 1$ & $\phi(m) \mid \phi(n)$.

<u>Case 2</u> $m > 1$.

Let $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$
be the prime factorization of m so that
each $a_j \geq 1$ $(1 \leq j \leq r)$.
Then by uniq. factorization
$$n = \left(p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}\right) c$$
where $(m, c) = 1$ & each $b_j \geq a_j$ $(1 \leq j \leq r)$.

$$\phi(m) = (p_1^{a_1} - p_1^{a_1 - 1})(p_2^{a_2} - p_2^{a_2 - 1}) \cdots (p_r^{a_r} - p_r^{a_r - 1})$$
$$= \left(p_1^{a_1 - 1} p_2^{a_2 - 1} \cdots p_r^{a_r - 1}\right)(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)$$
$$\phi(n) = \left(p_1^{b_1 - 1} p_2^{b_2 - 1} \cdots p_r^{b_r - 1}\right)(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)\,\phi(c)$$
since ϕ is mult. & $((p_1^{b_1} \cdots p_r^{b_r}), c) = 1$.

$$\phi(n) = \phi(m)\,\phi(c) \cdot (p_1^{b_1 - a_1} \cdots p_r^{b_r - a_r})$$
&

$\phi(m) \mid \phi(n)$ since each $b_j - a_j \geq 0$
& $\phi(c)(p_1^{b_1 - a_1} \cdots p_r^{b_r - a_r}) \in \mathbb{Z}$.

(ii) The converse of (i) is not true.
For example, $\phi(3) = 2 = \phi(6)$
so $\phi(6) \mid \phi(3)$ but $6 \nmid 3$.

7. SEE 2009 EXAM

8. (i) SEE 2009 EXAM

(ii) Let $p = 5$ & so $\frac{p-1}{2} = 2$.

x	$x^2 \pmod 5$
± 1	1
± 2	4

Hence 1, 4 are the quadratic residues mod 5.

(iii) SEE

(iv) $115 = 5 \cdot 23$ & so

$$\left(\frac{115}{131}\right) = \left(\frac{5}{131}\right)\left(\frac{23}{131}\right)$$

$\left(\frac{5}{131}\right) = \left(\frac{131}{5}\right)$ (By the Law of Quadratic Reciprocity since $5 \equiv 1 \pmod 4$)

$= \left(\frac{1}{5}\right)$ (since $131 \equiv 1 \pmod 5$)

$= 1.$

$\left(\frac{23}{131}\right) = -\left(\frac{131}{23}\right)$ (By the Law of Quadratic Reciprocity since $131 \equiv 23 \equiv 3 \pmod 4$)

$= -\left(\frac{16}{23}\right)$ (since $131 = 5(23) + 16$)

$= -1$ since $16 = 4^2$.

Hence $\left(\frac{115}{131}\right) = \left(\frac{5}{131}\right)\left(\frac{23}{131}\right) = (1)(-1) = -1.$

9(i) Let p be an odd prime.
Suppose $a \in \mathbb{Z}$, $1 \le a \le p-1$ &
a' is the multiplicative inverse of a mod p;
ie $aa' \equiv 1 \pmod{p}$.

Then clearly $p \nmid a'$ (otherwise $0 \equiv 1 \pmod{p}$ which is impossible).

$$\left(\frac{aa'}{p}\right) = \left(\frac{1}{p}\right) = 1 \quad \text{since } aa' \equiv 1 \pmod{p}.$$

$$\left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right) \text{ \&}$$

$$\left(\frac{a}{p}\right)\left(\frac{a'}{p}\right) = 1$$

$$\left(\frac{a}{p}\right)\left(\frac{a'}{p}\right)^2 = \left(\frac{a'}{p}\right) \text{ \&}$$

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right) \quad \text{since } \left(\frac{a'}{p}\right) = \pm 1 \text{ \& } \left(\frac{a'}{p}\right)^2 = 1.$$

(ii)

$$\left(\frac{1\cdot 2}{p}\right) + \left(\frac{2\cdot 3}{p}\right) + \cdots + \left(\frac{(p-2)(p-1)}{p}\right)$$

$$= \sum_{a=1}^{p-2} \left(\frac{a\cdot(a+1)}{p}\right)$$

$$= \sum_{a=1}^{p-2} \left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right)$$

$$= \sum_{a=1}^{p-2} \left(\frac{a'}{p}\right)\left(\frac{a+1}{p}\right)$$

(by (i), where a' is the multiplicative inverse of a mod p).

(p-8)

$$= \sum_{a=1}^{p-2} \left(\frac{a'(a+1)}{p} \right)$$

$$= \sum_{a=1}^{p-2} \left(\frac{aa' + a'}{p} \right)$$

$$= \sum_{a=1}^{p-2} \left(\frac{a'+1}{p} \right)$$

$$= \sum_{j=2}^{p-1} \left(\frac{j}{p} \right)$$

(since if $1 \leq a \leq p-2$ then $1 \leq a' \leq p-2$ since the multiplicative inverse of $p-1$ is $p-1$ since $p-1 \equiv (-1) \pmod{p}$)

$$= \left(\sum_{j=1}^{p-1} \left(\frac{j}{p} \right) \right) - \left(\frac{1}{p} \right)$$

$$= 0 - \left(\frac{1}{p} \right)$$

(By a homework problem)

$$= -1.$$