MATH 307 TEST 1

Please show your work. Enjoy! There are at least 150pts to earn here.

(25pts) Solve 2 of the problems on this page. Do not work more than 2, you need the time remaining for the rest of the test. Thanks.

Problem 1 How many positive integers between 1 and 221 are relatively prime to 221?
Hint: $221 = (13)(17)$.

Problem 2 Find the Egyptian fraction presentation of $\frac{20}{13}$.

Problem 3 Find the continued fraction form of $\frac{99}{26}$.

P1 $\phi(221) = \phi(13)\,\phi(17)$: (13, 17 are prime, hence $\gcd(13,17) = 1$)

$= (12)(16)$

$= \boxed{192}$

P2 $\frac{20}{13} = 1 + \underbrace{\frac{7}{13}}_{\frac{14}{26}} = \boxed{1 + \frac{1}{2} + \frac{1}{26}}$ also $\frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{26}$

many answers possible.

P3 $\frac{99}{26} = 3 + \frac{1}{\frac{26}{21}} = 3 + \frac{1}{1 + \frac{5}{21}} = 3 + \frac{1}{1 + \frac{1}{\frac{21}{5}}} = *$

$* = \boxed{3 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{5}}} = \frac{99}{26}}$

(25pts) Solve 2 of the problems on this page. Do not work more than 2, you need the time remaining for the rest of the test. Thanks.

Problem 4 Express 101 in its base-two representation. Then, for $m \in \mathbb{Z}$, show how we can calculate m^{101} from the value 1 by successive multiplications by m and squaring. Loosely, your exponentiation should not have more than about 10 steps.

Problem 5 Calculate the least positive residue of 50^{201} mod 33.

Problem 6 Find the last two digits of $5 \cdot 33^{7,000,321} \cdot 3^{7,000,322}$. Hint: $99 = 3 \cdot 33$.

P4 $101 = 64 + 32 + 4 + 1 = 1\cdot 2^6 + 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2 + 1\cdot 2^0$

$$101 = (1\,1\,0\,0\,1\,0\,1)_2$$

$1 \xrightarrow{m} m \xrightarrow{s} m^2 \xrightarrow{m} m^3 \xrightarrow{s} m^6 \xrightarrow{s} m^{12} \xrightarrow{s} m^{24} \xrightarrow{m} m^{25} \xrightarrow{s} m^{50} \xrightarrow{s} m^{100} \xrightarrow{m} m^{101}$

In other words

$$m^{101} = \Big[\Big[\Big(\big(\big((m)^2 m\big)^2\big)^2\Big)^2 m\Big]^2\Big]^2 m$$

(s: squared; m: multiply by m.)

//

P5 Euler Th^{m} is helpful! $\phi(33) = \phi(3\cdot 11) = \phi(3)\phi(11) = 2(10) = 20$.

Note $a^{\phi(33)} \equiv 1 \mod 33$ for $a \neq 0$. Hence,

$$50^{201} \equiv 50^{200}\,50 = (50^{20})^{10}\,50 \equiv 1^{10}\,50 \mod 33$$
$$\equiv 50 \mod 33$$
$$\equiv \boxed{17} \mod 33$$

(Or, $[50^{201}]_{33} = [17]$.)

P6
$$5\cdot 33^{7,000,321}\cdot 3^{7,000,322} = 5\cdot(3)\cdot(33)^{7000321}\,3^{7000321}$$
$$= 15\,(99)^{7,000,321}$$
$$\equiv 15\,(-1)^{7000321} \mod 100$$
$$\equiv -15 \mod 100$$
$$\equiv 85 \mod 100$$

But $\underbrace{a_r 10^r + \cdots + a_2 \times 10^2}_{\equiv 0 \mod 100} + \underbrace{a_1 \times 10 + a_0 \times 1}_{\text{last two digits}} \equiv a_1(10) + a_0 \Rightarrow \boxed{85}$ $\quad (\equiv \text{mod } 100)$

(25pts) Solve 2 of the problems on this page. Do not work more than 2, you need the time remaining for the rest of the test. Thanks.

Problem 7 Find $m, n \in \mathbb{Z}$ such that $gcd(131, 30) = m(131) + n(30)$. Also, calculate $[30]^{-1}$ in $\mathbb{Z}_{131}^{\times}$.

Problem 8 Find all integer solutions of $2x + 3y = 20$.

Problem 9 Simultaneously solve the system of congruences:

$$x \equiv 3 \pmod 5 \quad \& \quad x \equiv 4 \pmod{17}.$$

P7

$(131, 30) = (a, b)$

$(30, 11) = (b, a - 4b)$

$(11, 8) = (a - 4b, \; b - 2(a-4b)) = (a-4b, \; 9b - 2a)$

$(8, 3) = (9b - 2a, \; a - 4b - (9b - 2a)) = (9b - 2a, \; 3a - 13b)$

$(3, 2) = (3a - 13b, \; 9b - 2a - 2(3a - 13b)) = (3a - 13b, \; -8a + 35b)$

$(2, 1) = (-8a + 35b, \; 3a - 13b - (-8a + 35b)) = (-8a + 35b, \; 11a - 48b)$

Hence $1 = 11(131) - 48(30) \Rightarrow \boxed{m = 11, \; n = -48}$

$\Rightarrow \boxed{[30]_{131}^{-1} = [-48]_{131} = [83]_{131}}$

P8 Find $\mathbb{Z}$-sol^{n}s of $2x + 3y = 20$

$(-1)(2) + (1)(3) = 1$

Note, $\gcd(2,3) = 1 \mid 20 \;\therefore$ sol^{n}s exist. Moreover, $3 - 2 = 1$ suggests $2(-20) + 3(20) = 20 \;\therefore\; x_0 = -20, \; y_0 = 20$ is a particular sol^{n}. We then find the remaining sol^{n}s to this linear Diophantine Eq^{n} by the standard theorem, for each $t \in \mathbb{Z}$,

$$\boxed{x = -20 + 3t, \quad y = 20 - 2t}$$

P9 $x \equiv 3 \mod 5 \Rightarrow x = 3 + 5j$ for some $j \in \mathbb{Z}$

Thus $x \equiv 4 \mod 17 \Rightarrow 3 + 5j \equiv 4 \mod 17 \Rightarrow 5j \equiv 1 \mod 17$.

Notice, $(17, 5) = (a, b)$

$(5, 2) = (b, a - 3b)$

$(2, 1) = (a - 3b, \; b - 2(a - 3b))$

$1 = 7b - 2a = 7(5) - 2(17)$

$\rightarrow 7(5j) \equiv 7 \mod 17$

$\therefore j \equiv 7 \mod 17$

P9 continued,

$j \equiv 7 \mod 17$ & $x = 3 + 5j$ for some $j \in \mathbb{Z}$

$j = 7 + 17k$ for some $k \in \mathbb{Z}$

$\Rightarrow \quad x = 3 + 5(7 + 17k)$

$\therefore x = 38 + 85k$ for some $k \in \mathbb{Z}$

$\therefore \boxed{x \equiv 38 \mod 85}$

//

Alternate Sol'n:

$M = 85 = m_1 m_2 = 5(17)$

$M_1 = \frac{M}{m_1} = m_2 = 17$, $[M_1]_5^{-1} = [17]_5^{-1} = [2]_5^{-1} = [3]_5 \therefore y_1 = 3$

$M_2 = \frac{M}{m_2} = m_1 = 5$, $[M_2]_{17}^{-1} = [5]_{17}^{-1} = [7]_{17} \therefore y_2 = 7$

By Chinese Remainder Th^{m} we find,

$x \equiv 3(17)(3) + 4(7)(5) \mod 85$

$x \equiv 153 + 140 \mod 85$

$\boxed{x \equiv 38 \mod 85}$

(25pts) Solve 2 of the problems on this page. Do not work more than 2, you need the time remaining for the rest of the test. Thanks.

Problem 10 Find the order of 10 modulo 41. What is the signifcance of your result as you compare the order to the decimal expansion of 1/41 ? (use your calculator to see the expansion)

Problem 11 Let $b \in \mathbb{N}$ and suppose that $\gcd(b+18, b)$ is even and divisible by an odd prime. List the possible values for $\gcd(b+18, b)$.

Problem 12 Recall the base-eight representation of a number:

$$(c_d \dots c_2 c_1 c_0)_8 = c_d \times 8^d + \cdots c_2 \times 8^2 + c_1 \times 8 + c_0 \times 1$$

where $0 \leq c_0, c_1, \dots, c_d \leq 7$. Is $(7654321)_8$ divisible by 9 ?

P10

$10^2 = 100 \equiv 18 \mod 41$

$10^4 \equiv 18^2 = 324 \equiv 37 \equiv -4 \mod 41$

$10^5 \equiv -4(10) \equiv -40 \equiv 1 \mod 41 \quad \therefore \quad \boxed{\text{order}_{41}(10) = 5}$

$\frac{1}{41} = 0.\overline{02439\,02439\dots} = 0.\overline{02439}$ ← the period of the expansion is 5 digits.

– (this is no accident) –

P11

$\gcd(b+18, b)$ is even $\Rightarrow 2 \mid \gcd(b+18, b)$.

Observe $b+18$ and b are both divided by $\gcd(b+18, b)$

That is; $\gcd(b+18, b) \mid b+18$ AND $\gcd(b+18, b) \mid b$. Set $d = \gcd(b, b+18)$

Hence $d \mid b+18$ and $d \mid b \Rightarrow d \mid (b+18-b) \Rightarrow \underline{d \mid 18}$.

Thus $1 \leq d \leq 18$. Hence, as $2 \mid d$ and $d \mid 18$ we select from $d = 1, 2, 3, 6, 9, 18$. However, only $\boxed{d = 6 \text{ or } d = 18}$ are divisible by 3 and even.

P1a $8 \equiv -1 \mod 9$

$8^2 \equiv 1 \mod 9$

$8^3 \equiv -1 \mod 9$

etc.

$$(7654321)_8 = 1 + 2\cdot 8 + 3\cdot 8^2 + 4\cdot 8^3 + 5\cdot 8^4 + 6\cdot 8^5 + 7\cdot 8^6$$

$$\equiv 1 - 2 + 3 - 4 + 5 - 6 + 7 \mod 9$$

$$\equiv 4 \mod 9$$

Thus $(7654321)_8 \not\equiv 0 \quad \therefore \quad 8 \nmid (7654321)_8$.

– (this is the BASE-8 analog to the ± divisibility by 11 question for BASE-10) –

For example:

$(121)_{10}$ divisible by 11?

$$121 = 1\times 10^2 + 2\times 10 + 1$$

$$\equiv +1 - 2 + 1 \mod 11$$

$$\equiv 0 \mod 11 \quad (\text{of course } 121 = 11^2)$$

To be clear: from here on out, attempt all the problems you can. Thanks!

Problem 13 (10pts) Let $a, b, c, d \in \mathbb{Z}$ and $a \mid b$ and $c \mid d$. Prove that $ac \mid bd$.

Suppose a/b and c/d. Thus, $\exists j, k \in \mathbb{Z}$ such that $b = ja$ and $d = kc$. Consider,

$$bd = (ja)(kc) = (jk)(ac)$$

and $jk \in \mathbb{Z} \Rightarrow ac \mid bd$. //

Problem 14 (10pts) Prove that the product of successive integers is even. (I expect a proof referencing integers and precise definitions) consecutive

Let $a \in \mathbb{Z}$ then $a+1$ is the next integer. If $a \in 2\mathbb{Z}$ then $a = 2j$ for some $j \in \mathbb{Z}$ hence $a+1 = 2j+1$ and we find $a(a+1) = 2j(2j+1) = 2[j(2j+1)] \Rightarrow 2 \mid a(a+1)$ hence $a(a+1)$ is even. Otherwise, $a \in 2\mathbb{Z}+1$ hence $a = 2j+1$ for some $j \in \mathbb{Z}$ thus $a+1 = (2j+1)+1 = 2j+2$. Therefore,

$$a(a+1) = (2j+1)(2j+2) = 2[(2j+1)(j+1)] \Rightarrow 2 \mid a(a+1).$$

Thus, as $\mathbb{Z} = 2\mathbb{Z} \cup (2\mathbb{Z}+1)$ we've covered all cases and we conclude $a(a+1)$ is even for all $a \in \mathbb{Z}$.

Problem 15 (10pts) Suppose $[a] \in \mathbb{Z}_n$ has order $k > 1$. Furthermore, suppose $b \in \mathbb{Z}$ has $ab \equiv 1 \bmod(n)$. Prove $[b]$ also has order k.

If $[a]$ has order $k > 1$ then $[a]^k = [1]$ and $[a]^l \neq [1]$ for $1 \leq l < k$. We are given $ab \equiv 1 \bmod(n)$ hence $[a][b] = [1]$. Notice, $([a][b])^k = [a]^k [b]^k = [b]^k \Rightarrow \underline{[b]^k = [1]}$.

Suppose $[b]^j = [1]$ for $1 \leq j < k$ then $([a][b])^j = [1]^j$

$\Rightarrow [a]^j [b]^j = [1] \Rightarrow [a]^j [1] = [1] \Rightarrow [a]^j = [1]$

which contradicts the order of a being $k > j$. Thus $[b]^j \neq [1]$ for $1 \leq j < k$ yet $[b]^k = [1]$ thus order of $[b]$ is also k.

Problem 16 (5pts) Arrange the following list of mathematicians in chronological order from ancient to modern: Gauss, Dirichlet, Diophantus, Euclid, Euler, Sprano :

Euclid < Diophantus < Euler < Gauss < Dirichlet < Sprano

Problem 17 (10pts) Consider $G = (\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$ where the multiplication is defined modulo 5. Fill out the following multiplication table:

$(\mathbb{Z}_5)^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Define $H = \{1, 4\}$. Show how G is partitioned by the cosets of H.

pick anything not in H, $2H = \{2, 8\} = \{2, 3\}$

$H \cup 2H = \{1, 4\} \cup \{2, 3\}$ [OR $H \cup 3H$, diff. representative same coset OR $4H \cup 3H$ or $4H \cup 2H$]

Problem 18 (15pts) State and prove Lagrange's Theorem.

Lagrange's Th^m

Let H be a subgroup of a finite group G then the order of H divides the order of G.

aka Let G be a group with $|G| < \infty$ then $H \leq G \Rightarrow |H| \mid |G|$.

Proof: found many places.
(In particular, see Lecture 4 page 5.)