15
10
10
15
20
15
15
5

190

S-155

Take-Home #3
Due January 8, 1968

Wou may use Ore, McCoy, your notes, and the computer, Hut no other sources and no discussion of the exam outside class will Hbe allowed.

10 ✓ 1. (10 points) Let $r(n)$ denote the total number of solutions (proper and improper) of the equation $x^2+y^2=n$ and let $R(N)=\sum_{n\le N} r(n)$. Show that $R(N)$ is related to the number of integral lattice points on and within a certain circle and use this fact to prove that

$$\pi(N-2\sqrt{2N}+2) < R(N) \le \pi(N+2\sqrt{2N}+2)$$

$$\pi(\sqrt{N}-\sqrt{2})^2 \qquad \pi(\sqrt{N}+\sqrt{2})^2$$

10 ✓ 2. (10 points) Let $x=\langle 1,1,1,\ldots\rangle$. Show that the sequence $\{q_k\}$ of denominators of the convergents of x may be defined recursively by $q_1=q_2=1$, $q_{n+1}=q_n+q_{n-1}$. Verify that

$$q_n=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

3. (15 points) Use the theory of continued fractions (and the computer) to find a solution of the simultaneous congruences

$$409x \equiv 661 \pmod{988027}$$
$$463x \equiv 870 \pmod{410531}$$

15 ✓ 4. (15 points) Find all (if any) integral lattice points on the ellipse $10x^2-8xy+5y^2=100$.

15 ✓ 5. (15 points) Given that $2.7182 < e < 2.7183$, show that the first 8 partial quotients of e are 2,1,2,1,1,4,1,1. What reduced rational number with denominator no greater than 50 best approximates e ?

2500
7149927

6. (20 points) Farmer Jones has 14299853 orange trees which he plans to plant in two square orchards of unequal size. If he desires to minimize the total number of rows in his orchards, how many trees should he plant in each orchard ?

7. (25 points) If $p = 4K+1$ is a prime, show that

$$\sum_{k=1}^{K} [\sqrt{pk}] = \frac{p^2-1}{12}$$

Hint: count the lattice points above the parabola $y^2 = px$ in a suitable rectangle.

8. (15 points) Show that 3413 is a prime; show that its smallest primitive root is 2; and find the quadratic residues of 3413.

9. (50 points) Theorem If $n \mid K^2+3$, where n is odd and $(3,n) = 1$, then there exist integers s and t such that $n = t^2+3s^2$.

Prove the above theorem by completing the following steps.

10. i) Show that there exist integers r, s such that

$$\left| \frac{K}{n} - \frac{r}{s} \right| \leq \frac{1}{(N+1)s} \qquad 0 < s \leq N$$

10. ii) Show that if $t = Ks - rn$, then $t^2+3s^2 \equiv 0 \pmod{n}$ and

$$t^2+3s^2 < \frac{n^2}{N^2} + 3N^2 .$$

10. iii) Use differential calculus to find the real number $x_0 > 0$ which minimizes the function $F(x) = \frac{n^2}{x^2} + 3x^2$, and show that when $N = [x_0]$ we have

$$t^2+3s^2 < 2\sqrt{3}\, n$$

iv) Conclude from iii) that $t^2+3s^2 = n$, $2n$, or $3n$, and eliminate the undesirable cases to complete the proof of the theorem.

10 v) Use the theorem to show that there are an infinite number of primes of the form $3n+1$.

$r_1 = 3$

$r_2 =$

10. (15 points) Define the sequence r_n recursively as follows: $r_1 = 3$, $r_{n+1} = r_n^2 - 2$. Then the following theorem provides a useful test for the primality of the so-called Mersenne numbers:

$31 = 4(7)+3$

don't have to prove Mersenne primes prime.

Theorem: If $p = 4n+3$ is a prime and $M_p = 2^p - 1$, then M_p is a prime if and only if $r_{p-1} \equiv 0 \pmod{M_p}$.

Assuming the truth of the above theorem, or otherwise, determine whether or not $2^{31} - 1$ is a prime.

S-155
Quiz #5

32

Closed book
40 minutes

Name Steve Bellenot

1. (10 points) Decide whether $x^2 \equiv 150 \pmod{1009}$ is solvable or not. You may use the fact that 1009 is a prime.

10

$2 \cdot 3 \cdot 5^2$

$$\left(\frac{150}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right)\left(\frac{5^2}{1009}\right) = 1 \left(\frac{3}{1009}\right) 1 = \left(\frac{1009}{3}\right)$$

$$= \left(\frac{1}{3}\right) = 1 \quad \text{IT IS}$$

2. (15 points) Find all solutions of the congruence $x^2 \equiv 5 \pmod{\cancel{164}}$. $2^2 \cdot 41$

82
123
164

12

$x^2 \equiv 5 \bmod 164 \iff x^2 \equiv 5 \bmod 2^2 \ \& \ x^2 \equiv 5 \bmod 41$

$$\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1$$

$x \equiv 1$ ✓ mod 4 $\qquad x \equiv 13$ ✓ mod 41

$x \equiv -1 \quad 3 \qquad x \equiv -13 \quad 28$

$M_1 = 41 \qquad M_2 = 4 \qquad M_1T_1 \equiv 1 \bmod 4$

$T_1 = 1 \qquad T_2 = -10 \qquad M_2T_2 \equiv 1 \bmod 41$

$x \equiv 1 \cdot 41 \cdot 1 + (-10) \cdot 4 (13) \equiv -89 \equiv 75$ (mod 164)

$x \equiv -41 + (-10) \cdot 4 (13) \equiv -171 \equiv 157$

$x \equiv 41 \cdot 1 + (-10) \cdot 4 (-13) \equiv 171 \equiv 7$

$x \equiv -41 + (-10) \cdot 4 (-13) \equiv 89$

$x \equiv 7$ ← clearly wrong

$x \equiv 75$

$x \equiv 89$

$x \equiv 157$

mod 164 are all solutions

13 clearly is one solution

3. (20 points) Show that $x^2 \equiv 11 \pmod{p}$ has a solution if and only if $p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44}$.

10

$p = m(44) + r$ r must be odd

$p=2$ $\left(\frac{11}{p}\right) = \left(\frac{11}{2}\right) = \left(\frac{1}{2}\right) = 1$ $p=2$ has solution

$$\left(\frac{11}{p}\right) = \left(\frac{11}{m(44)+r}\right) = \left(\frac{m(44)+r}{11}\right)(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}\left(\frac{4m+r}{11}\right)$$

$p=1$ $\left(\frac{11}{1}\right) = \left(\frac{0}{1}\right) = 1$ sol

$p=3$ $\left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1$ no sol

$p=2n$ $\left(\frac{11}{2n}\right) =$ ~~I must assume p is odd prime~~ $\Rightarrow$ or $p=2$ works

or otherwise $p=10$ has the sol $x \equiv 1 \bmod 10 \Rightarrow x^2 \equiv 11 \bmod 10$

$p=5$ $\left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$ sol

$p=7$ $\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2^2}{7}\right) = 1$ sol

$p=9$ $\left(\frac{11}{9}\right) = \left(\frac{2}{9}\right) = 1$ sol

$p=11$ $\left(\frac{11}{11}\right) = \left(\frac{0}{11}\right) = 1$ sol

$p=13$ $\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1$ no sol

$p=15$ $\left(\frac{11}{15}\right) \Leftrightarrow \left(\frac{11}{3}\right)$ & $\left(\frac{11}{5}\right)$ $\left(\frac{11}{3}\right) = -1$ no sol

$p=17$ $\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = -1$ no sol

$$\cancel{\left(\frac{11}{p}\right) = \left(\frac{11}{44m+r}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{44m+r}{11}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{4m+r}{11}\right)}$$

$p=19$ $\left(\frac{11}{19}\right) = -\left(\frac{19}{11}\right) = -\left(\frac{8}{11}\right) = -\left(\frac{2^2}{11}\right)\left(\frac{2}{11}\right) = 1$ sol

$p=21$ $\left(\frac{11}{21}\right) \Leftrightarrow \left(\frac{11}{3}\right)$ & $\left(\frac{11}{7}\right)$ $\left(\frac{11}{3}\right) = -1$ no sol

$p=23$ $\left(\frac{11}{23}\right) = -\left(\frac{23}{11}\right) = -\left(\frac{1}{11}\right) = -1$ no sol

$p=25$ $\left(\frac{11}{25}\right) \Leftrightarrow \left(\frac{11}{5}\right) = 1$ sol

$p=27$ $\left(\frac{11}{27}\right) \Leftrightarrow \left(\frac{11}{3}\right) = -1$ no sol

$p=29$

165

S-155
Take-Home Exam #4
Due January 22, 1968

Ore
McCoy

10
10
10
15
5
20
20
20
20
10
140

10 1. (10 points) Prove that at least one of the integers in a Pythagorean triple must be divisible by 5.

10 2. (10 points) Prove that the product of two consecutive integers cannot be a power of an integer.

10 3. (10 points) Prove that if $\alpha = \langle a_0, \overline{1, 1, 1, 1, 1, 2a_0} \rangle$, then α^2 is not an integer.

15 4. (15 points) Show that if $a > 1$ and a is odd, then $\sqrt{a^2 - 4} = \langle a - 1, \overline{1, \tfrac{1}{2}(a - 3), 2, \tfrac{1}{2}(a - 3), 1, 2a - 2} \rangle$

5. (15 points) Prove that there are infinitely many primes whose last (decimal) digits are 3.

20 6. (20 points) Find all positive integers x such that x^x ends in 3. (e.g. $7^7 = 1509543$)

20 7. (20 points) Let $n = 4^{\ell}(8k + 7)$, where k and ℓ are non-negative integers. Prove that n cannot be represented as the sum of three squares.

8. (20 points) Given that $(366)^2 + (393)^2 = (519)^2 + (138)^2 = 288405$, express 288405 as a product of prime powers and find all positive integral solutions of $x^2 + y^2 = 288405$.

540

↑ beware this mutha
—Fowler

9. (20 points) A certain control room contains n meters numbered $1, 2, \ldots, n$, each of which may be engaged of disengaged at the discretion of the operator. Each meter is originally engaged and set at zero. The meters measure the effect of a sequence of n operations $T_1, T_2, \ldots, T_n$ whereby with T_k , $1 \leq k \leq n$, the condition of being engaged or disengaged is reversed and the reading is increased by k units for those meters and only those meters whose number is divisible by k.

Thus, if the m^{th} meter has a reading of A units and is engaged after T_{k-1} and if $k \mid m$, then after operation T_k , it is disengaged and has a reading of A + k units, while if $k \nmid m$, it is engaged and still has a reading of A units.

Show that a meter is both engaged and has an odd numerical reading after all n operations have been completed if and only if its number is double a perfect square.

10. (25 points) Prove that the equation $x^y - y^x = 1$ has precisely two solutions in positive integers and find them.

$(x, y) = /$

$x =$ any no.
$y = 0$

$\boxed{\begin{matrix} x = 2 \\ y = 1 \end{matrix}}$ $\boxed{\begin{matrix} x = 3 \\ y = 2 \end{matrix}}$

one of x & y is odd

$\cancel{x^y = y^x + 1}$

$y^x = x^y - 1$

$y^x = (x-1)\underbrace{(x^{y-1} + x^{y-2} + \ldots x + 1)}_{y \text{ terms}}$

$y \mid (x-1)$ or $y \mid$ ———

$y^x > x^y$

if $ky+1 = x$

$(ky+1)^y - y$

$ky+1$

$y^{y+a} = (y+a)^y - 1$

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

since y is even $[(y+a)^n]^2 - 1$

S-155
Take-Home Exam #1
Due October 30, 1967

Unlimited time. You may use McCoy and Ore and your notes, but no other sources. Naturally no discussion of the exam outside class shall be allowed.

83

150 total points

1. (10 points) Show that there are infinitely many primes of the form $6n+5$.

10

2. (10 points) If a, m, and n are positive integers and $m \neq n$, show that
$$\text{g.c.d.}\left(a^{2^m}+1,\ a^{2^n}+1\right) = \begin{cases} 1 & \text{if } a \text{ is even} \\ 2 & \text{if } a \text{ is odd} \end{cases}$$

10

3. (10 points) Let $S = \{1, 2, \ldots, n\}$. If 2^k is the integer in S which is the highest power of 2, prove that 2^k is not a divisor of any other member of S.

10

4. (10 points) Prove there are infinitely many primes by considering the sequence
$$2^2+1,\ 2^4+1,\ \ldots,\ 2^{2^k}+1,\ \ldots$$

10

5. (15 points) Let φ denote the Euler function and let n be a fixed positive integer. Show that the equation $\varphi(x) = n$ has only a finite number of solutions. Find all solutions of $\varphi(x) = 24$, and find the smallest n such that $\varphi(x) = n$ has no solution.

10

6. (15 points) Find all solutions of the congruence
$$x^3 + x \equiv 0 \pmod{918}$$

0

$(p-1)^2((p-1)!)$ $(p-1)^3 \times p^{k-1}$

7. (20 points) If n is a positive integer, prove that $(n-1)!+1$ is a power of n if and only if $n = 2, 3$, or 5.

10

8. (20 points) If $n > 1$, prove that $\sum_{j=1}^{n} \frac{1}{j}$ is not an integer. 2^k $4p^2+1$

5

9. (20 points) Prove that there are infinitely many primes of the form $4n+1$.

0

10. (20 points) If n is a positive integer, prove that $\frac{(2n)!}{(n!)^2}$ is an even integer.

20

$2 - 1$	$3 - 2$	$5 - 4$	$\boxed{7} - 6$	$11 - 10$
$2^2 - 2$	$\boxed{3^2} \ 6$	$5^2 - 20$	$7^2 - 42$	
$2^3 - 4$	$3^3 - 18$	$13 - 12$	$17 - 16$	$19 - 18$
$2^4 - 8$		$23 - 21$	$27 - 26$	
$2^5 - 16$				

S-155
Quiz #1
October 6, 1967

Closed book
20 minutes
20 points

Name STEVE BELLENOT

20

The Whig Party wishes to collect $1000 at a fund raising banquet and to minimize the cost of the meal. If each man who attends is charged $19 and each woman, $13, what is the smallest number of meals that must be prepared? If at least 20 women must be invited to the banquet, then what is the smallest number of meals that the Whigs must whip up?

START HERE →

$$\boxed{19x + 13y = 1000}$$

$(19, 13) = 1$

$19 = 13 + 6$

$13 = 2(6) + 1$

$1 = 13 - 2(6)$

$1 = 13 - 2(19 - 13)$

$1 = 3(13) - 2(19)$

$1000 = 3000(13) - 2000(19)$

A sol $x_0 = -2000$

$y_0 = 3000$

gen sol

$x = x_0 + \frac{b}{d} t$

$y = y_0 - \frac{a}{d} t$

$x = -2000 + 13t$

$y = 3000 - 19t$

$13 \overline{)2000}$ = 154; 13, 70, 65, 50

$154 \times 13 = 462 + 154 = 2002$

$154 \times 19 = 1386 + 154 = 2926$

ANOTHER FORM gen sol

$x = 2 + 13t \qquad y = 74 - 19t$

All Pos integers sol are

MEN	WOMEN	TOTAL MEALS
2	74	76
15	55	70
28	36	64
41	17	58

✓

58 is the smallest no. of meals
with 17 for women 41 for men

64 is the smallest no of meals ✓
with the condition $y \geq 20$

$74 \times 13 = 222 + 74 = 962$; $962 + 38 = 1000$

$19 \times 41 = 19 + 76 = 779$; $13 \times 17 = 51 + 17 = 221$; $779 + 221 = 1000$

(189) [249] Course grade A+

S-155
Part II

Open book, notes
Three hours.

Name STEVE BELLENOT

II Intermediate problems.

1. (15 points) Prove that $n^5 \equiv n \pmod{30}$ for every integer n.

(15)

$\Leftrightarrow$ $n^5 = n \mod 2$ $\quad$ $n^5 = n \mod 3$ $\quad$ $n^5 = n \mod 5$

$n=0$, $n=1$ true $\quad$ $n=0$ true, $n=1$ true, $n=2$ true $\quad$ true for all n

Since it is true for all these values, the use of Chinese Remainder theorem will give $2 \cdot 3 \cdot 5 = 30$ solutions $\therefore$ it is true for all n mod 30

2. (15 points) Prove that 19 does not divide any number of the form $4n^2 + 4$, where n is an integer.

(15)

49 64
38 57
81 100
76 95

If $19 \mid 4n^2+4 \Rightarrow 4(n^2+1) \equiv 0 \mod 19$

Quadratic residues (19) are $\{0, 1, 4, 9, 16, 6, 17, 11, 7, 5\}$ 68

72

Residues n^2+1 are $\{1, 2, 5, 6, 7, 10, 12, 17, 18, 8\}$

Residues $4(n^2+1)$ are $\{4, 8, 1, 5, 9, 2, 10, 11, 15, 13\}$

$\therefore 4(n^2+1) \not\equiv 0 \mod 19$ & $19 \nmid 4(n^2+1)$

show $\left(\frac{-4}{19}\right) = -1$

3. (15 points) Let $L = \langle a_0, a_1, \ldots, a_n \rangle$. Is it true that $\langle a_0, a_1, \ldots, a_n, a_{n+1} \rangle = L + \frac{1}{a_{n+1}}$? Explain.

(12)

not necessarily true for

$$L + \frac{1}{a_{n+1}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{a_n}}} + \frac{1}{a_{n+1}} \neq a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{a_n + \cfrac{1}{a_{n+1}}}}}$$

why not? explain

(counterexample)

4. (15 points) Prove that no four consecutive integers can be powers of positive integers (even with different exponents).

0

assume opposite $a = w^n$ $a+1 = x^m$ $a+2 = y^l$ $a+3 = z^k$

$a+1-a = x^m - w^n = 1 = z^k - y^l = a+3-(a+2)$

$\Rightarrow x^m + y^l = w^n + z^k$

not too fruitful an approach

5. (15 points) Find all positive integers n such that $\varphi(2n) = \varphi(3n)$.

15

$\phi(2n) = 2n\left(1-\frac{1}{2}\right)\prod_{p|n}\left(1-\frac{1}{p}\right) = \phi(3n) = 3n\left(1-\frac{1}{3}\right)\prod_{p|n}\left(1-\frac{1}{p}\right)$

or $n = 2n\left(1-\frac{1}{2}\right) = 3n\left(1-\frac{1}{3}\right) = 2n$ no cases

if $2|n$ but $3\nmid n$ $\quad n = 2n\frac{1}{2}$ all cases

if $3|n$ but $2\nmid n$ $\quad \frac{2}{3}n = 2n$ no cases

if $2|n$ & $3|n$ $\quad \frac{2}{3}n = n$ no cases

Solution n is a solution if $2|n$ & $3\nmid n$ ✓

6. (15 points) Prove that every positive integer greater than 11 is the sum of two composite numbers. (Hint: choose your representation so that one of the composite numbers is always 6 or 9.)

15

Let n be a integer greater than 11

if n is even $\quad n = 6 + (n-6)$ since $n-6$ is even and > 5 it is composite

if n is odd $\quad n = 9 + (n-9)$ since $n-9$ is even and > 2 it is composite ✓

7. (15 points) If $x^2 + y^2 = z^2$, show that $xyz \equiv 0 \pmod{60}$.

15

From last take home we know 5 divides one of x, y or z

If z is odd z^2 is odd so both $x^2 + y^2$ can't be odd so x, or y is even thus $2 | x, y$ or z. ~~Quadratic residues mod 4 are $\{0, 1\}$ if $z^2 \equiv 1$ the one of x^2 or $y^2 \equiv 0$~~. Quadratic residues mod 3 are $\{0, 1\}$ so if $z^2 \equiv 1 \Rightarrow$ one of x^2 or $y^2 \equiv 0$ thus $3 | x, y$ or z.

Quadratic residues mod 8 are $\{0, 1, 4\}$ thus $z^2 \not\equiv 4$ & if $z^2 \equiv 1$ One of $x^2, y^2 \equiv 0$ $8 | x^2, y^2$ or $z^2 \Rightarrow 4 | x, y$ or z

$xyz \equiv 0 \mod 60$ since $5, 4, 3$ divide xyz

8. (15 points) If $p > 3$, show that the sum of the quadratic residues of p is divisible by p.

15

$$\sum_{i=0}^{\frac{p-1}{2}} i^2 = \frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)\left(2\left(\frac{p-1}{2}\right)+1\right)}{6}$$

since this term $= p$ the

all quadratic residues mod p

$p | \sum i^2$ unless $p | 6$ $\therefore$

if $p > 3$ $p |$ sum quadratic residues.

$$\frac{1}{1} \quad \frac{5}{3} \quad \frac{14}{6} \quad \frac{30}{10}$$

$$1 \quad \frac{5}{3} \quad \frac{7}{3} \quad \frac{9}{3}$$

$$\sum_{1}^{n} i = \frac{n(n+1)(2n+1)}{6}$$

$$\frac{\Sigma}{\Sigma} = \frac{2i+1}{3} \quad \frac{n(n+1)}{2}$$

9. (15 points) ~~Show that if p is a prime, the congruence $x^9 \equiv 10 \pmod p$ is always solvable.~~ 3 is a primitive root of any prime of form 2^n+1 $n>1$ ✓

2

All we must show is $3^{2^i} \not\equiv 1 \mod 2^n+1 \ (0 < i < n-1)$

if untrue $3^{2^i} - 1 \equiv 0 \mod 2^n+1$

$3^2 = 9 = 2^3+1$

10. (15 points) Find a general form for the continued fraction expansion of a number of the form $\sqrt{4a^2+4}$, where a is a positive integer.

15

$$2a < \sqrt{4a^2+4} < 2a+1$$

k	0	1	2	3
r_k	0	$2a$	$2a$	$2a$
s_k	1	4	1	4
α_k	$[\sqrt{4a^2+4}]$	$\left[\frac{\sqrt{4a^2+4}+2a}{4}\right]$	$[\sqrt{4a^2+4}+2a]$	$\left[\frac{\sqrt{4a^2+4}+2a}{4}\right]$
a_k	$2a$	a	$4a$	a

✓

thus $\sqrt{4a^2+4} = \langle 2a, \overline{a, 4a} \rangle$

4
15
8
120
105
225

165

S-155
Take-home Exam #2
Due November 21, 1967

You may use any source you wish, but naturally no discussion of the exam outside class shall be allowed.

10 1. (10 points) What day of the week was August 20, 1921 ?

10 2. (10 points) Prove that the congruence $x^8 \equiv 16 \pmod{p}$ is solvable, where p is a prime.

$2^{\frac{p-1}{2}} \equiv 1$ $\quad x^2 \equiv 2 \bmod p$ is sol.

10 3. (10 points) Solve the congruence $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}$ (11·13)

15 4. (15 points) Solve the congruence $3x^4 + 2x^3 - 6x^2 - 4x \equiv 0 \pmod{3352}$ $(2^3 \cdot 419)$

15 5. (15 points) If $(a,b) = 1$, prove that any segment of length $\sqrt{a^2 + b^2}$ on the line $ax + by = c$ contains at least one integral lattice point.

$\frac{x}{bc} + \frac{y}{ac} = 1$

15 6. (15 points) Let p be an odd prime. If a,b,c are integers and if $(a,p) = 1$, show that the parabola $ax^2 + bx + c = py$ passes through an infinite number of integral lattice points if and only if $b^2 - 4ac$ is either zero or a quadratic residue modulo p.

75

20 7. (20 points) The positive integer N is called a perfect number if it is the sum of all its positive divisors other than itself--e.g. 6 and 8128. It has long been known that all even perfect numbers are of the form $2^{p-1}(2^p - 1)$, where both p and 2^{p-1} are primes (see Ore, pg. 91).

No odd perfect number has ever been found, but if such a number does exist, prove that it must be of the form $D = q^{4m+1} K^2$, where q is a prime of the form $4k+1$ and $(K,q) = 1$. Use this fact to prove that if $D \equiv 3 \pmod{4}$, then D cannot be perfect.

95

15

110 8. (20 points) If $(a,8) = 1$, prove that there are infinitely many primes of the form $8n + a$.

9. (25 points) Let $N = 17^{19} + 1$. Show that any odd prime which divides N must be of one of the forms $34k \pm 3$; $34k \pm 7$; $34k \pm 11$; or $34k \pm 5$. Using Fermat's technique (Ore, pg. 60) or any other method, attempt to represent N as the product of prime powers.

Ore

~~10.~~ (25 points) Each classroom at Hardly Normal College has the same number of rows of desks as there are desks in each row and is always filled with students. During the annual May Frolic, the English class combined with the calculus class to play several games, and it was found that one, two, and three students, respectively, were left over when the group broke up into teams to play bridge, baseball, and basketball. Finally, to cap off the day's festivities, the cream of the calculus class athletes defeated an English class team in a game of football, even though the English class rooting section was slightly more than four times as large as that of the calculus class. How many students were there in each class ?

.25

C = no Cal E = no E C = 16 E = 25

both are sq. $C = x^2$ $E = y^2$

$C + E \equiv 1 \mod 4$ $4(C+11) < E - 11$

$C + E \equiv 2 \mod 9$

$C + E \equiv 3 \mod 5$

1 odd, 1 even

$4C < E + 33$

$C + E = 4k^2 + 4l^2 + 4l + 1$

$C + E = 5m + 4 + 5j + 4$ exact one of m & j is odd

$10a + 4 + 10b + 5 + 4 \equiv 1 \mod 4$

$2a + 2b \equiv 0 \mod 4$

$E + C = 4k + 1 + 4l + 1$

1	1
2	4
3	4
4	1

mod 5

C	E
0	3
3	0
$\boxed{4}$	$\boxed{4}$

mod 9

C	E
~~0~~	2
$\boxed{1}$	$\boxed{1}$
~~2~~	0
~~3~~	8
$\boxed{4}$	$\boxed{7}$
~~5~~	6
~~6~~	5
$\boxed{7}$	$\boxed{4}$
~~8~~	3

$0^2 \equiv 0$ $6^2 \equiv 0$
$1^2 \equiv 1$ $7^2 \equiv 4$
$2^2 \equiv 4$ $8^2 \equiv 1$
$3^2 \equiv 0$ $9^2 \equiv 0$
$4^2 \equiv 7$
$5^2 \equiv 7$

484, 1849

~~16~~	49
~~16~~	
~~64~~	169
$\boxed{64}$	$\boxed{289}$
144	

~~49~~	~~324~~
~~169~~	784
~~289~~	1444
~~324~~	1369
$\boxed{484}$	1849

S-155
Supplementary Notes

<u>Theorem</u> The equation $x^4+y^4=z^4$ is not solvable in non-zero rational integers.

Proof: It suffices to show that there is no primitive solution of $x^4+y^4=z^2$.
Suppose x, y, and z form a solution of the latter equation. Without loss of generality we may assume that $x>0$, $y>0$, $z>0$, and y even. [Why must either x or y be even?]
Since $(x^2)^2+(y^2)^2=z^2$, we have

$$x^2=a^2-b^2,\quad y^2=2ab,\quad z=a^2+b^2$$

where $(a,b)=1$ and exactly one of a and b is odd. If a were even, we would have

$$1\equiv x^2=a^2-b^2\equiv -1 \pmod 4).$$

Consequently, b is even. Now we analyze the solutions of $x^2+b^2=a^2$. There exists integers p and q where $(p,q)=1$, $p>0$, $q>0$, and not both of p and q are odd such that

$$x = p^2 - q^2 \qquad b = 2pq \qquad a = p^2 + q^2$$

from $y^2 = 2ab$ we obtain $y^2 = 4pq(p^2+q^2)$.

Since p, q, p^2+q^2 are relatively prime in pairs, each of these numbers must be a perfect square — thus there exist integers r, s, t such that $p = r^2$, $q = s^2$, $p^2+q^2 = t^2$.

It follows that $r^4 + s^4 = t^2$; $x = r^4 - s^4$;

$y = 2rst$; $z = a^2 + b^2 = r^8 + 6r^4s^4 + s^8$.

Therefore, $z > (r^4+s^4)^2 = (t^2)^2$, or $t < z^{1/4}$.

Thus if one solution of $x^4 + y^4 = z^2$ were known, another solution r, s, t could be found for which $r > 0$, $s > 0$, $t > 0$ and $0 < t < z^{1/4}$, but this would give an infinite decreasing sequence of positive integers, which is clearly impossible. This completes the proof of the theorem.

S-155

Supplementary Notes

<u>Theorem</u> All solutions of the equation $x^y = y^x$ in rational numbers x, y with $y > x > 0$ are given by $x = \left(1 + \frac{1}{n}\right)^n$, $y = \left(1 + \frac{1}{n}\right)^{n+1}$ where n is a positive integer.

Proof: Suppose that x, y is such a solution and that $y > x$. Then $r = x/y-x$ is a positive rational number and ~~that~~ $y = (1 + \frac{1}{r})x$. Thus, we have $x^y = x^{(1+\frac{1}{r})x}$ and since $x^y = y^x$ we also have $x^{(1+\frac{1}{r})x} = y^x$. This shows that $x^{1+\frac{1}{r}} = y = (1+\frac{1}{r})x$. Hence, $x^{\frac{1}{r}} = 1 + \frac{1}{r}$, and we obtain

$$x = \left(1 + \frac{1}{r}\right)^r \qquad y = \left(1 + \frac{1}{r}\right)^{r+1}$$

Now, let $r = \frac{n}{m}$, where $(m, n) = 1$ and $x = t/s$, where $(t, s) = 1$. Since $x = \left(1 + \frac{1}{r}\right)^r$, we have $\left(\frac{m+n}{n}\right)^{\frac{n}{m}} = \frac{t}{s}$ and therefore, $\frac{(m+n)^n}{n^n} = \frac{t^m}{s^m}$.

(cont'd)

Note that $(m+n, n) = 1$ since $(m, n) = 1$. Therefore, $((m+n)^n, n^n) = 1$ and since $(t^m, s^m) = 1$ also, we have $(m+n)^n = t^m$ and $n^n = s^m$. Since $(m, n) = 1$, there exist positive integers k and l such that $(m+n) = k^m$; $t = k^n$; $n = l^m$; and $s = l^n$. Therefore, $m + l^m = k^m$, which implies that $k \geq l+1$. If $m > 1$, we would have $k^m > (l+1)^m \geq l^m + ml^{m-1} + 1 > l^m + m = k^m$, which is impossible. Thus, $m = 1$ and $r = n$.

We conclude that

$$(1) \qquad x = \left(1 + \frac{1}{n}\right)^n \qquad y = \left(1 + \frac{1}{n}\right)^{n+1}$$

where n is a positive integer, as desired.

Conversely, if x and y satisfy (1), then $x^y = y^x$ since $n\left(1+\frac{1}{n}\right)^{n+1} = (n+1)\left(1+\frac{1}{n}\right)^n$.

Note: if we are only seeking integral solutions, it is easy to show that $x = 2$, $y = 4$ is the only such solution for $x^y = y^x \Rightarrow x^{\frac{1}{x}} = y^{\frac{1}{y}}$, but $\sqrt[3]{3} > \sqrt[2]{2} = \sqrt[4]{4} > \sqrt[5]{5} > \sqrt[6]{6} > \dots > \sqrt[1]{1}$.

Theorem The equation $x^2+16=y^3$ has no solution in integers x, y.

Proof: If x were even, then y would also be even — say $x=2x_1$, $y=2y_1$. Hence, $x_1^2+4=2y_1^3$, and consequently x_1 would be even. Thus, $x_1=2x_2$ and we have $2x_2^2+2=y_1^3$. Therefore, $y_1=2y_2$, and $x_2^2+1=4y_2^3$ which is impossible.

Therefore, x must be odd, and consequently $y^3\equiv 1 \pmod 8$. This means that $y\equiv 1 \pmod 8$, and $y-2\equiv -1 \pmod 8$. Since $y-2 \mid y^3-8=x^2+8$, the number x^2+8 has a divisor of the form $8t-1$. It follows that x^2+8 has a prime divisor p either of the form $8k+5$ or of the form $8k+7$. However,

$$\left(\frac{-8}{p}\right)=\left(\frac{8}{p}\right)=\left(\frac{2}{p}\right)=-1 \quad \text{if } p\equiv 5$$

and

$$\left(\frac{-8}{p}\right)=-\left(\frac{8}{p}\right)=(-1)(1)=-1 \quad \text{if } p\equiv 7.$$

It follows that no integral solutions exist.

<u>Theorem</u> The problem of solving the equation $(u-v)^5 = u^3 - v^3$ in positive integers u, v with $u > v$ reduces to that of solving the equation $(x+1)^3 - x^3 = y^2$ in positive integers.

Proof: Suppose $(x+1)^3 - x^3 = y^2$. Then, putting $u = y(x+1)$ and $v = yx$, we obtain $u - v = y$ and $u^3 - v^3 = y^3[(x+1)^3 - x^3] = y^5 = (u-v)^5$.

Conversely, if $\overset{u,v}{\cancel{x,y}}$ satisfy the equation $(u-v)^5 = u^3 - v^3$ and if $v < u$, then putting $y = (u,v)$, $x = \frac{v}{y}$, $t = u/y$, we have $(x,t) = 1$ and since $u > v$, it follows that $t > x$.

Therefore, $y^5(t-x)^5 = y^3(t^3 - x^3)$ or

$$y^2(t-x)^4 = (t^3 - x^3)/t - x = (t-x)^2 + 3tx,$$

and it follows that $(t-x)^2 \mid 3tx$. Hence, since $(t,x) = 1$, we obtain $t - x = 1$, and consequently, $t = x+1$, $u = y(x+1)$, and $y^2 = (x+1)^3 - x^3$

<u>Theorem</u> The product of any three consecutive positive numbers cannot be a power with exponent greater than 1 of a positive integer.

Proof: Suppose there exist n, k and $s > 1$ such that $n(n+1)(n+2) = k^s$. Since $(n+1, n(n+2)) = 1$, it follows that there exist positive integers a, b such that $n+1 = a^s$ and $n(n+2) = b^s$. Consequently, $1 = (n+1)^2 - n(n+2) = (a^2)^s - b^s$, which is impossible.

<u>Theorem</u> There exists an infinite sequence of positive integers $a_1, a_2, \ldots$ such that each of the numbers $a_1^2 + a_2^2 + \ldots + a_n^2$, where $n = 1, 2, \ldots$ is the square of a positive integer.

Proof: We use induction on n. Suppose for n, numbers $a_1, a_2, \ldots, a_n$ exist so that $a_1^2 + a_2^2 + \ldots + a_n^2$ is the square of an <u>odd</u> positive integer > 1 — i.e. $a_1^2 + a_2^2 + \ldots + a_n^2 = (2k+1)^2$.

(cont'd)

Then, using the identity $(2k+1)^2 + (2k^2+2k)^2 = (2k^2+2k+1)^2$

and putting $a_{n+1} = 2k^2+2k$ we obtain

$$a_1^2 + a_2^2 + \dots + a_{n+1}^2 = (2k^2+2k+1)^2$$

which again is the square of an odd positive integer.

- - - - - - - - - - - - - - - - - - -

for example, $3^2+4^2=5^2$; $3^2+4^2+12^2=13^2$;

$3^2+4^2+12^2+84^2=85^2$; $3^2+4^2+12^2+84^2+3612^2=3613^2$.

- - - - - - - - - - - - - - - - - - -

Several Interesting Results

1. There are no three squares which form an arithmetic progression and for which the common difference is a square.

2. There are no two positive integers such that the sum and difference of their squares are squares.

3. For every positive integer n there exist n Pythagorean triangles with different hypotenuses and the same area.

4. There are no cubes of three different positive integers which form an arithmetic progression.

5. If n is a positive integer >1, then the number $1^3+2^3+\dots\dots n^3$ is not the cube of a positive integer.