

MATH 104B, PRACTICE MIDTERM 2 SOLUTIONS, WINTER 2003.

1. Determine which numbers in the list 700, 270, $22100 = 2 \times 5 \times 13 \times 17$ can be written as a sum of two squares, and write those that can be as sums of two squares.

Solution. Now $700 = 2^2 \cdot 5^2 \cdot 7$ but $7 \equiv 3 \pmod{4}$ occurs to an odd power, so 700 is not a sum of two squares.

$270 = 2 \cdot 5 \cdot 3^3$ and 3 occurs to an odd power, so 270 is not a sum of squares.

22100 is a sum of squares because there are no primes in the factorization which are congruent to 3 modulo 4.

Now $2 \cdot 5 = 10 = 1^2 + 3^2$ and $13 = 2^2 + 3^2$ and $17 = 4^2 + 1^2$, so

$$22100 = (1 + 3i)(1 - 3i)(2 + 3i)(2 - 3i)(4 + i)(4 - i).$$

Now $(1 + 3i)(2 + 3i) = -7 + 9i$ and so $(1 + 3i)(2 - 3i)(4 + i) = (-7 + 9i)(4 + i) = -37 + 29i$. Hence $22100 = 37^2 + 29^2$.

2. Prove that $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/2}$.

Solution. Using Gauss's Lemma, $\left(\frac{2}{p}\right) = (-1)^n$ where n is the number of elements in the set $S = \{2, 4, 6, \dots, (p-1)\}$ which are negative when expressed in the absolute least residue system modulo p . This equals the number of elements of S in the interval $(p/2, p)$, that is the number of even integers in $(p/2, p)$. This equals the number of integers in $(p/4, p/2)$ which is $\lfloor p/2 \rfloor - \lfloor p/4 \rfloor$. If $p = 8k + r$ then

$$\lfloor p/2 \rfloor - \lfloor p/4 \rfloor = \lfloor 4k + r/2 \rfloor - \lfloor 2k + r/4 \rfloor = \lfloor r/2 \rfloor - \lfloor r/4 \rfloor + 2k.$$

Hence

$$\left(\frac{2}{p}\right) = (-1)^n = (-1)^{\lfloor r/2 \rfloor - \lfloor r/4 \rfloor} = \begin{cases} 1 & r = 1, 7 \\ -1 & r = 3, 5 \end{cases} = (-1)^{(p^2-1)/8}.$$

3. Describe the primes p which divide $x^2 + 5$ for some value of x .

Solution. $p|x^2 + 5$ for some x if and only if $\left(\frac{-5}{p}\right) = 1$ or 0 . Now it equals zero if and only if $p = 5$. We determine the primes where it equals 1.

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (-1)^{(p-1)/2} \left(\frac{p}{5}\right).$$

For the numbers relatively prime to 20 we compute

k	1	3	7	9	-9	-7	-3	-1
$(-1)^{(p-1)/2} \equiv k \pmod{4}$	1	-1	-1	1	-1	1	1	-1
$k \pmod{5}$	1	3	-3	-1	1	3	-3	1
$\left(\frac{p}{5}\right)$	1	-1	-1	1	1	-1	-1	1
$(-1)^{(p-1)/2} \left(\frac{p}{5}\right)$	1	1	1	1	-1	-1	-1	-1

We see that a prime p divides $x^2 + 5$ for some x if and only if p is congruent to one of 1, 3, 7, 9 modulo 20.

4. Suppose that a_1, \dots, a_k are positive numbers and define $C_k = [a_0, \dots, a_k]$. Show that $C_k = p_k/q_k$ where for $k \geq 3$, p_k and q_k satisfy $p_k = a_k p_{k-1} + p_{k-2}$ and $q_k = a_k q_{k-1} + q_{k-2}$. (*)

Solution.

$$C_0 = \frac{a_0}{1}, \quad C_1 = \frac{a_0 a_1 + 1}{a_1}, \quad C_2 = a_0 + \frac{1}{a_1 + 1/a_2} = \frac{a_0(a_1 + 1/a_2) + 1}{a_1 + 1/a_2} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1}.$$

We see that taking

$$p_0 = a_0, \quad p_1 = a_0 a_1 + 1, \quad p_2 = a_0 a_1 a_2 + a_0 + a_2$$

and

$$q_0 = 1, \quad q_1 = a_1, \quad q_2 = a_1 a_2 + 1,$$

that the equations (*) hold for $k = 2$. Now assume they hold for $k < n$. Then

$$\begin{aligned} C_n &= [a_0, \dots, a_n] = [a_0, \dots, a_{n-2}, a_{n-1} + 1/a_n] = \frac{(a_{n-1} + 1/a_n)p_{n-2} + p_{n-3}}{(a_{n-1} + 1/a_n)q_{n-2} + q_{n-3}} \\ &= \frac{a_n a_{n-1} p_{n-2} + a_n p_{n-3} + p_{n-2}}{a_n a_{n-1} q_{n-2} + a_n q_{n-3} + q_{n-2}} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}. \end{aligned}$$

Hence the equations hold for $k = n$, and by induction they hold for all values of $k \geq 2$.

5. For the fraction $61/19$, calculate the continued fraction and all the convergents, and solve the diophantine equation $61x - 19y = 1$.

Solution.

$$61 = 3 \cdot 19 + 4$$

$$19 = 4 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

So

$$\frac{61}{19} = [3, 4, 1, 3].$$

Convergents are

$$\frac{3}{1}, \quad \frac{13}{4}, \quad \frac{16}{5}, \quad \frac{61}{19}.$$

So

$$61 \cdot 5 - 19 \cdot 16 = (-1)^2 = 1.$$