MATH 115B SOLUTIONS III
MAY 1, 2007

(1) Establish each of the following assertions:

(a) Each of the integers 2^n where $n = 1, 2, \ldots$, is a sum of two squares.

(b) If $n \equiv 3$ or $6 \pmod 9$, then n cannot be represented as a sum of two squares.

(c) Every Fermat number $F_n = 2^{2^n} + 1$, where $n \geq 1$ can be expressed as a sum of two squares.

Solution:

(a) If n is odd, then

$$2^n = (2^{(n-1)/2})^2 + (2^{(n-1)/2})^2,$$

while if n is even, then $2^n = (2^{n/2})^2 + 0^2$ for $n \geq 1$.

(b) Suppose that $n \equiv 3$ or $6 \pmod 9$. Since $a^2 \equiv 0, 1, 4$ or $7 \pmod 9$ for any integer a it follows that $a^2 + b^2 \equiv 0, 1, 2, 4, 5, 7$ or $8 \pmod 9$. Hence n is not a sum of two squares.

(c) For a Fermat number F_n, where $n \geq 1$,

$$F_n = 2^{2^n} + 1 = (2^{2^{n-1}})^2 + 1^2.$$

(2) Show that a positive integer n is a sum of two squares if and only if $n = 2^m a^2 b$, where $m \geq 0$, a is an odd integer, and every prime divisor of b is of the form $4k + 1$.

Solution:

Suppose that $n = 2^m a^2 b$, where $m \geq 0$, a is odd and every prime divisor of b is of the form $4k+1$. If m is even, then $n = (2^{m/2}a)^2 b$, and so, from a theorem proved in class (which one?), it follows that n is a sum in two squares. If m is odd, then $n = (2^{(m-1)/2})^2(2b)$, and so we can again apply the theorem alluded to above.

(3) Find a positive integer having at least three different representations as the sum of two squares. [Hint: Choose an integer that has three distict prime factors, each of the form $4k + 1$.]

Solution:

Recall that we have the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

We may apply this identity to, for example, $1105 = 5 \cdot 13 \cdot 17$. Then

$$\begin{aligned}
1105 &= 5(3^2 + 2^2)(4^2 + 1^2) = 5(14^2 + 5^2) \\
&= (2^2 + 1^2)((14^2 + 5^2) = 33^2 + 4^2; \\
1105 &= 13(2^2 + 1^2)(4^2 + 1^2) = 13(9^2 + 2^2) \\
&= (3^2 + 2^2)(9^2 + 2^2) = 31^2 + 12^2; \\
1105 &= 17(2^2 + 1^2)(2^2 + 3^2) = 17(7^2 + 4^2) \\
&= (4^2 + 1^2)(7^2 + 4^2) = 32^2 + 9^2.
\end{aligned}$$

(4) If the positive integer n is not the sum of two squares of integers, show that n cannot be represented as the sum of two squares of rational numbers.

Solution:

Suppose that n is not a sum of two squares. Then (from a theorem discussed in class), there is a prime $p \equiv 3 \pmod 4$, and an odd integer k satisfying $p^k \mid n$ and $p^{k+1} \nmid n$. If n could be written as a sum of squares of two rational numbers, say $n = (a/b)^2 + (c/d)^2$, then $n(bd)^2 = (ad)^2 + (bc)^2$. Thus, $n(bd)^2$ is a sum of two squares. However, in the prime factorisation of $n(bd)^2$, the prime p occurs to an odd power, and this contradicts the theorem alluded to above.

(5) Prove that the positive integer n has as many representations as the sum of two squares as does the integer $2n$. [Hint: Starting with a representation for n as a sum of two squares, obtain a similar representation for $2n$, and conversely.]

Solution:

Let $n = a^2 + b^2$ for integers a and b. Then $2n = (a + b)^2 + (a - b)^2$, and so there is a representation of $2n$ as a sum of two squares.

Suppose conversely that $2n = c^2 + d^2$. Since c and d are both even or both odd, it follows that $c - d$ and $c + d$ are even integers. Hence $n = [(c + d)/2]^2 + [(c - d)/2]^2$.

(6) Prove that of any four consecutive integers, at least one of them is not representable as a sum of two squares.

Solution:

Given any four consecutive integers, one of them, say n, satisfies $n \equiv 3 \pmod 4$. Write $n = N^2m$, where m is squarefree, and $N^2 \equiv 1 \pmod 4$. Then m is divisible by a prime of the form $4k + 3$, and so n cannot be written as a sum of two squares.

(7) For any $n > 0$, show that there is a positive integer that can be expressed in n distinct ways as a difference of two squares. [Hint: Note that, for $k = 1, 2, \ldots, n$,

$$2^{2n+1} = (2^{2n-k} + 2^{k-1})^2 - (2^{2n-k} - 2^{k-1})^2.]$$

Solution:

For any $n > 0$ and $k = 1, 2, \ldots, n$, we have

$$(2^{2n-k} + 2^{k-1})^2 - (2^{2n-k} - 2^{k-1})^2 = 4 \cdot 2^{2n-k} \cdot 2^{k-1} = 2^{n+1}.$$

Thus 2^{n+1} has n representations as a difference of two squares.