Homework 6 (due Thursday, March 31), in class,  
(or up to 3pm in the box outside of 3086EH)

You should look at Niven, Zuckerman and Montgomery, Chap. 3.4–3.6, and satisfy 
yourself that you understand the material. Then hand in the following.

1. Suppose \( a \) is a quadratic nonresidue of each of the odd primes \( p \) and \( q \).

   (a) Determine the Jacobi symbol \( \left( \frac{a}{pq} \right) \).

   (b) Is \( x^2 \equiv a \pmod{pq} \) solvable or unsolvable? [Give an explanation.]

   (c) Suppose an odd number \( a > 1 \) is not a perfect square. Show that there exist two 
distinct odd primes \( p \) and \( q \) such that \( a \) is a quadratic nonresidue modulo \( p \) and also 
modulo \( q \).

   [Hint: For (c) use the reciprocity law for the Jacobi symbol, to reduce to finding a 
suitable odd integer \( R \) with \( \left( \frac{R}{a} \right) = -1 \). Then prove suitable such \( R \) exist.]

2. Determine all the odd prime numbers which can be expressed in the form

\[
f(x, y) = x^2 + xy + 5y^2,
\]

for integral \((x, y)\).

3. Determine all the positive integers that can be represented in the form

\[
f(x, y) = x^2 - y^2,
\]

for integral \((x, y)\).

4. Let \( 0 = s_1 < s_2 < \cdots \) be the set of integers of the form \( x^2 + y^2 \), for integral \((x, y)\). 
Show that there exist arbitrarily large gaps between some successive terms of \( s_n \), i.e.

\[
\limsup_{n \to \infty} (s_n - s_{n-1}) = +\infty.
\]

5. Suppose that \( p \geq 7 \) is a prime. Show that

\[
\left( \frac{n}{p} \right) = \left( \frac{n + 1}{p} \right) = 1
\]

for at least one number in the set \( \{1, 2, \ldots, 9\} \).
6. (a) Prove that when $n$ is a positive integer, then $n$ and $2n$ have the same number of representations as a sum of two squares.

(b) Does the same hold for proper representations?

7. Consider the binary quadratic form $f(x, y) = 4x^2 + 17xy + 20y^2$.

(a) Find a reduced form equivalent to $f(x, y)$.

(b) Find the least positive integer that can be expressed $n = f(x, y)$ for integer $(x, y)$.

8. Prove that if a positive integer can be expressed as a sum of squares of two rational numbers, then it can be expressed as a sum of squares of two integers.

9. Do exactly one of the three problems (a)-(c).

(a) Show that all prime factors $p$ of each integer $n^4 - n^2 + 1$ must be congruent to 1 modulo 12.

(b) Show that if for $n > 1$ the $n$-th Fermat number $F_n = 2^{2^n} + 1$ is a prime $F_n = p$, then 3, 5 and 7 are all primitive roots modulo $p$.

(c) Show that $\frac{x^2 - 2}{2y^2 + 3}$ is never an integer when $x$ and $y$ are integers.

10. Let $d(n)$ denote the number of (positive) divisors of $n$. Thus $d(6) = 4$.

(a) Show that $d(n)$ is a multiplicative function, and compute $d(p^j)$ for $p$ a prime, $j \geq 1$.

(b) Prove that there is a constant $C$ such that

$$d(n) \leq \exp(C \frac{\log n \log \log n}{\log \log n})$$

holds for $n \geq 3$. Thus it follows that for each $\epsilon > 0$ there is a constant $C_{\epsilon} > 0$ such that

$$d(n) \leq C_{\epsilon} n^\epsilon$$

holds for all $n \geq 2$.

[Hint: Obtain an upper bound for the number of primes that divide $n$ as being $\leq C_1 \frac{\log n \log \log n}{\log \log n}$.]