1. Assignment 5

(due on Thursday, May 7 by 2PM)

**Policy:** You may collaborate with your classmates and you are allowed to consult books while solving the homework problems. However you should not consult any other people (except the instructor and TA) or use internet resources such as online forums. Please cite book references if any are used. If you use results not proved in class please provide your own proof.

1. (a) Implement a function \( \text{qr}(n, p) \) which takes inputs \( n \) an integer and \( p \) a prime, and returns:

\[
\begin{cases} 
1 & \text{if } n \neq 0 \text{ and } n \text{ is a quadratic residue mod } p \\
-1 & \text{if } n \text{ is a quadratic non-residue mod } p \\
0 & \text{if } n = 0.
\end{cases}
\]

In Sage, you can test your function against the built-in function \texttt{kroncker}(n, p).

(b) Using Sage, for example, make a table of quadratic non-residues modulo primes \( p \) up to 1000. For each such \( p \), compute \( \sqrt{p} \) and the maximal length \( \ell_{ns}(p) \) of consecutive integers \( n \) which are quadratic non-residues mod \( p \). For which \( p \) does \( \ell_{ns}(p) \) exceed \( \sqrt{p} \)? (If you make the table in the Sage notebook interface, the output will be too long to fit in one window, so you’ll get a link to a text file. Print out this file and turn it in along with your code.)

2. (a) Find all primes \( p \) such that

\[ x^2 \equiv 23 \pmod{p} \]

is solvable.

(b) Use Gauss’ Lemma to determine if the congruence

\[ x^2 \equiv a \pmod{1016} \]

is solvable in integers for \( a = 125 \) and \( a = 129 \).

(c) Let \( N = k^4 - k^2 + 1 \) with \( k \in \mathbb{Z} \). Show, using the Legendre symbol, that if \( p | N \) then \( p \equiv 1 \pmod{12} \). \textit{(Hint: Rearrange the terms in two different ways)}

(d) Show that there are infinitely many primes \( p \equiv 1 \pmod{3} \).
3.

(a) Prove that 18 is a primitive root mod 37. Is it a primitive root mod $37^2$?
Determine primitive roots mod $37^k$ for every $k \geq 2$.
(b) Show that for $h$ odd we have that $h^{2k-2} \equiv 1 \pmod{2^k}$ for $k \geq 3$.
(c) Consider the primitive root 3 of 17. Computing indices with respect to this
primitive root, find the solutions to the following congruences:

$$8x^5 \equiv 3 \pmod{17}$$
and
$$7x \equiv 4 \pmod{17}.$$ 

4.

(a) Let $p$ be an odd prime. Show that if $0 \leq n \leq p - 2$ then

$$\sum_{j=1}^{p} j^n \equiv 0 \pmod{p}.$$ 

(b) Let $p$ be an odd prime. Prove that for $m, n \in \mathbb{Z}$ with $(m, p) = 1$ and
$(n, p) = 1$ we have

$$\sum_{j=1}^{p} \left( \frac{mj^2 + n}{p} \right) = - \left( \frac{m}{p} \right).$$

Note that here $\left( \frac{a}{p} \right) = 0$ if $a \equiv 0 \pmod{p}$ and otherwise it is the usual
Legendre symbol. (Hint: Use Euler’s criterion. First prove the result
mod $p$.)

5.

(a) Let $m \in \mathbb{Z}_+$. Show that $m^3 - 5$ is never a perfect square. (Hint: Look mod
4.)

(b) Show that there are no integer solutions to

$$(x + y + z)^2 = (3k + 2)(xy + yz + xz).$$

(Hint: Let $p$ with $p \equiv 2 \pmod{3}$ a prime that appears at an odd power in
the prime factorization of $3k + 2$)