Number Theory, Fall 2016. Test #3 (revised).
Due on Friday, November 4th, by 1pm

Directions: Provide complete arguments (do not skip steps). State clearly and FULLY any result you are referring to. Partial credit for incorrect solutions, containing steps in the right direction, may be given. If you are unable to solve a problem (or a part of a problem), you may still use its result to solve a later part of the same problem or a later problem in the exam.

Rules: You may freely use your class notes, the class textbook by Jones and Jones, all materials from Math 5653 websites (Spring 2013, Spring 2014, Fall 2016), all publicly available materials from Math 3354 website from Spring 2016 as well as the following notes on Euclidean domain and Gaussian integers

`https://www.maths.nottingham.ac.uk/personal/cw/download/fnt_chap5.pdf`

You may also ask me any questions about the problems. You are NOT allowed to

(i) discuss midterm problems with anyone else except me

(ii) use any online resources except the ones mentioned above

(iii) use other books without obtaining a prior permission

Violation of any of the rules (i)-(iii) will be considered a violation of UVA honor code and appropriate action will be taken.

1. (12 pts) For each $r = 1, 5, 7$ and 11 prove that there are infinitely many primes of the form $12n + r$, with $n \in \mathbb{N}$. Five points for proving there are infinitely many primes of the form $12n + 1$ and seven points for the other three cases.

2. (8 pts) Let $\omega = \frac{1+\sqrt{5}}{2}$ and $R = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$. Prove that R is a Euclidean domain.

3. (10 pts) Find all integers (positive and negative) which are representable in the form $a^2 - 2b^2$ with $a, b \in \mathbb{Z}$. You may use without proof that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

4. (10 pts) As usual, for an integer $n > 1$, we denote by Q_n the group of quadratic residues mod n (thought of as a subgroup of U_n).

(a) Prove that if n is a prime power, then Q_n is always cyclic. **Hint:** This can be proved essentially without computations by citing suitable results from the book.

(b) Assume that n is divisible by two different primes of the form $4m+1$. Prove that Q_n is NOT cyclic.

(c) Let $p_1 = 4n_1 + 3, \ldots, p_k = 4n_k + 3$ be distinct primes such that the numbers $2n_1+1, \ldots, 2n_k+1$ are pairwise coprime, and let $n = p_1 \ldots p_k$. Prove that Q_n is cyclic.

(d) Prove that for any $k \in \mathbb{N}$, there exist k primes satisfying the hypothesis of (c). You are allowed to use the full statement of Dirichlet's theorem on primes in arithmetic progressions (not just the special cases we proved in class/homework) which says the following: let $a, b \in \mathbb{Z}$ be coprime (it is not required that a and b are positive). Then there are infinitely many primes of the form $am + b$ with $m \in \mathbb{Z}$.