Homework Assignment 1
Due Wednesday October 2

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2002**

Instructions: *Please work with others,* and acknowledge who you work with in your write up. If you can do a problem using a computer please do, but describe how you use the computer. For more practice you can do the problems in the book.

There are **six problems**.

1. (1 point each) Compute the following gcd's using the Euclidean algorithm (show the steps):

$$\gcd(7, 19), \quad \gcd(388, 32), \quad \text{and } \gcd(510, 900).$$

2. (2 points) Use the Euclidean algorithm to find integers x, $y \in \mathbb{Z}$ such that

$$123x + 567y = 6.$$

3. (2 points each) Let $R = \mathbb{Z}[\sqrt{-5}]$ be the ring of elements of the form $a + b\sqrt{-5}$ such that $a, b \in \mathbb{Z}$. An nonzero non-unit x in R is *irreducible* if the only divisors of x are of the form xu with u a unit. Also, the norm of $a + b\sqrt{-5}$ is

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2.$$

   (a) Find the units in R.

   (b) Prove that if $x, y \in R$ then $N(xy) = N(x)N(y)$.

   (c) Show that 2 is irreducible in the ring $\mathbb{Z}[\sqrt{-5}]$.
   [Hint: If $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ and take norms.]

   (d) Show that $(1 + \sqrt{-5})$ is irreducible in $\mathbb{Z}[\sqrt{-5}]$.
   [Hint: If $(1 + \sqrt{-5}) = (a + b\sqrt{-5})(c + d\sqrt{-5})$ and take norms.]

4. (4 points) Find the second smallest positive integer x such that

$$\begin{aligned} x &\equiv 1 \pmod 2, \\ x &\equiv 2 \pmod 3, \\ x &\equiv 3 \pmod 5, \\ x &\equiv 5 \pmod 7. \end{aligned}$$

5. (5 points) Suppose that $a, b \in \mathbb{Z}/n$, and let $\tilde{a}, \tilde{b} \in \mathbb{Z}$ be lifts of a, b, respectively. Prove that $\gcd(\tilde{a}, \gcd(\tilde{b}, n))$ doesn't depend on the choice of $\tilde{a}, \tilde{b}$.

6. (a) (2 points) Prove that $\varphi(n)$ is the number of units in $\mathbb{Z}/n$.

   (b) (4 points) Prove that φ is multiplicative as follows. Show that the natural map $\mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$ is an injective map of rings, hence bijective by counting, then look at unit groups.