

Name: Solutions

## Quiz 5

Math 74

November 1, 2006

1. State the definition of an ideal.

An ideal is a <sup>nonempty</sup> subset  $J \subseteq \mathbb{Z}$  such that:

(i) If  $a, b \in J$ , then  $a + b \in J$ ;

(ii) If  $a \in J$ , then  $-a \in J$ .

2. State the Euclidean algorithm.

Let  $m$  and  $n$  be integers (not both zero).

Then there exists  $a, b \in \mathbb{Z}$  such that

$$\gcd(m, n) = am + bn.$$

3. Let  $m, n \in \mathbb{Z}$  (not both zero). Use the Euclidean algorithm to show that  $m$  and  $n$  are relatively prime if and only if there exist  $a, b \in \mathbb{Z}$  such that  $am + bn = 1$ .

Suppose that  $\exists a, b \in \mathbb{Z}$  such that  $am + bn = 1$ . Let  $d$  be a common divisor of  $m$  and  $n$ . Then  $d \mid (am + bn)$ , so  $d \mid 1$ , so  $d = 1$ . Thus  $\gcd(m, n) = 1$ .

Suppose that  $\gcd(m, n) = 1$ . Then by the Euclidean Algorithm, there exists  $a, b \in \mathbb{Z}$  such that  $am + bn = 1$ .