

## MATH 521A: Abstract Algebra Exam 1

Please read the following instructions. For the following exam you are free to use a calculator and any papers you like, but no books or computers. Please turn in **exactly four** problems. You must do problems 1-3, and one more chosen from 4-6. Please write your answers on separate paper, make clear what work goes with which problem, and put your name or initials on every page. You have 50 minutes. Each problem will be graded on a 5-10 scale (as your quizzes), for a total score between 20 and 40. This will then be multiplied by  $\frac{5}{2}$  for your exam score.

### Turn in problems 1,2,3:

1. Richard Dedekind, a pioneer of ring theory, was born in 1831 and died in 1916. Use the Euclidean Algorithm to find  $\gcd(1831, 1916)$  and to express that gcd as a linear combination of 1831, 1916.
2. Let  $a, m, n \in \mathbb{N}$  with  $\gcd(m, n) = 1$ . Prove that  $mx \equiv a \pmod{n}$  has a solution  $x$ .
3. Let  $n \in \mathbb{N}$ , and suppose that  $[a]$  is a nonzero element of  $\mathbb{Z}_n$ . Prove that  $[a]$  is a unit if and only if  $[a]$  is *not* a zero divisor.

### Turn in exactly one more problem of your choice:

4. Let  $p$  be a positive prime. Use the Fundamental Theorem of Arithmetic to prove that there do not exist  $a, b \in \mathbb{N}$  with  $a^2 = pb^2$ .
5. Working in  $\mathbb{Z}_{21}$ , find the multiplicative inverse of  $[8]$ , and use this to solve the modular equation  $[8] \odot [x] = [13]$ .
6. Working in  $\mathbb{Z}_n$ , prove that the following holds for all  $[a], [b], [c], [d]$ :

$$([a] \oplus [b]) \odot ([c] \oplus [d]) = ([a] \odot [c]) \oplus ([a] \odot [d]) \oplus ([b] \odot [c]) \oplus ([b] \odot [d])$$

### You may also turn in the following (optional):

7. Describe your preferences for your next group assignment. (will be kept confidential)