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 six** problems. You must do problems 1-4, and two more chosen from 5-8. 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 75 minutes. Each problem will be graded on a 5-10 scale (as your quizzes), for a total score between 30 and 60. This will then be multiplied by $\frac{5}{3}$ for your exam score.

Turn in problems 1,2,3,4:

1. Let $p \in \mathbb{N}$ be irreducible, with $p > 4$. Use the Division Algorithm to prove that p is of the form $6k+1$ or $6k+5$ for some integer k.
2. Use the extended Euclidean Algorithm to find $\gcd(119, 175)$ and to find $x, y \in \mathbb{Z}$ with $119x + 175y = \gcd(119, 175)$.
3. Apply the Miller-Rabin test to $n = 63$ and $a = 2$, and interpret the result.
4. Let $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$. Without using the FTA, prove that $\gcd(a, b^2) = 1$.

Turn in exactly two more problems of your choice:

5. Prove that $S = \mathbb{N} \cup \{\pi\}$ is well-ordered.
6. Prove the following variant of the division algorithm: Let a, b be integers with $b > 0$. then there exist (not necessarily unique) integers q, r such that $a = bq + r$ and $-1 \leq r \leq b - 2$.
7. Let $a, b, c, d \in \mathbb{Z}$ with $a|c$, $b|c$, and $\gcd(a, b) = d$. Without using the FTA, prove that $ab|cd$.
8. Let $a, b, c \in \mathbb{Z}$ with $ab = c^2$ and $\gcd(a, b) = 1$. Prove that a, b are perfect squares.

You may also turn in the following (optional):

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