**Exam 2**
**Solutions**

Do each of the following (6 points each).

What does the expression '$a \equiv bn$' mean? In particular, what must $a$, $b$, and $n$ be for the expression to be meaningful?

Given $n \in -\{1\}$ and $a, b \in$, we say that '$a \equiv bn$' if $n|(b-a)$.

Define *relation*.

Given sets $S$ and $T$ a relation between $S$ and $T$ is a subset of $S \times T$.

State Fermat's Little Theorem.

Let $p \in$ be prime and $a \in$ an integer not congruent to zero modulo $p$. Then $a^{p-1} \equiv 1p$.

Four of the following seven assertions are false. In the space at the bottom of this page, identify three of them and give counterexamples. Note that you do not have to justify your counterexamples—only present them. (8 points each)

Given $a, b, c \in$ such that $a|bc$ it follows that $a|b$ or $a|c$.

False: e.g. a= 4, b=c=2.

Given $a, b \in$, there exists $m, n \in$ such that $am + bn = \gcd(a, b)$.

Every $\bar{a} \in_5 -\{\bar{0}\}$ has a multiplicative inverse.

If $a, b, k \in$ and $k$ divides an integer combination of $a$ and $b$, then $k|a$ and $k|b$.

False: e.g. if k=6, a = b = 3, then $k|(1 \cdot a + 1 \cdot b)$.

If $2x \equiv 04$, then $x \equiv 04$.

False: $x$ could also be 2.

If $a, b, k \in$ are integers such that $k$ divides $a + b$ and $a$, then $k$ divides $b$.

Let us say that two integers are related if the difference between the larger and the smaller of the two is prime. Then this defines an equivalence relation on . False: $2 \sim 5$ and $5 \sim 8$, but $2 \not\sim 8$, so transitivity fails.

Find the closest number $x \in$ to 100 such that

$$x \equiv 12, \quad x \equiv 13, \quad x \equiv 57.$$

Note that $x$ can be either greater or less than 100. (10 points)

Use the Euclidean algorithm to compute $k = \gcd(187, 255)$ and to express $k$ as an integer combination of 187 and 255. (15 points)

Given $a, b, n \in$ such that $\gcd(a, b) = 1$, show that $\gcd(na, nb) = n$. (10 points)

Clearly $n$ divides both $na$ and $nb$, so $n \leq \gcd(na, nb)$. On the other hand, because $\gcd(a, b) = 1$, there are integers $s, t \in$ such that

$$1 = sa + tb$$

Multiplying through by $n$ gives me

$$n = san + tbn = s(an) + t(bn).$$

That is, $n$ is an integer combination of $an$ and $bn$. Since all integer combinations of $an$ and $bn$ are multiples of $\gcd(an, bn)$, it follows that $n = k \gcd(an, bn)$ for some $k \geq 1$. In particular, $n \geq \gcd(an, bn)$.

In summary, I have shown that $\gcd(an, bn) \leq n \leq \gcd(an, bn)$. Therefore $\gcd(an, bn) = n$.

Prove that if $a, b \in$ are integers such that $4|(a^2 + b^2)$, then $a$ and $b$ are even. (15 points)

The hypothesis is that $4|(a^2 + b^2)$. In other words, $a^2 + b^2 \equiv 04$.

Suppose in order to obtain a contradiction, that either $a$ or $b$ is odd—for argument's sake, say $a$ is odd. Then $a$ is equivalent to 1 or 3 modulo 4. Either way $a^2 \equiv 14$.

Now $b$ can be either odd or even, so we need to rule out both possibilities. If $b$ is odd, then $b^2 \equiv 14$, and it follows that

$$a^2 + b^2 \equiv 1 + 1 \equiv 24,$$

contradicting the hypothesis. If $b$ is even, then $b$ is congruent to 0 or 2 modulo 4, so $b^2 \equiv 04$. Therefore

$$a^2 + b^2 \equiv 1 + 0 \equiv 14,$$

again contradicting the hypothesis.

So no matter what, $a$ cannot be odd. It follows that both $a$ and $b$ must be even.