MATH 255: ELEMENTARY NUMBER THEORY
EXAM #1

Problem 1.

(a) Compute $\gcd(24, 103)$.

(b) Find integers $x, y \in \mathbb{Z}$ such that $24x + 103y = 1$ and x is divisible by 5.

Solution. The Euclidean algorithm gives $103 = 4 \cdot 24 + 7$, $24 = 3 \cdot 7 + 3$ and $7 = 2 \cdot 3 + 1$, so $\gcd(24, 103) = 1$. For (b), we write

$$1 = 7 - 2 \cdot 3 = 7 - 2(24 - 3 \cdot 7) = 7 \cdot 7 - 2 \cdot 24 = 7(103 - 4 \cdot 24) - 2 \cdot 24 = -30 \cdot 24 + 7 \cdot 103$$

so $x = -30$ and $y = 7$ and indeed $5 \mid 30$.

Problem 2. For any integer $a \in \mathbb{Z}$, prove that $\gcd(3a + 5, a + 2) = 1$.

Solution. By Euler's lemma, we have

$$\gcd(3a + 5, a + 2) = \gcd(3a + 5 - 3(a + 2), a + 2) = \gcd(-1, a + 2) = 1.$$

Problem 3. Let $m \in \mathbb{Z}_{>0}$ be a positive integer. Show (by induction) that for all $n \in \mathbb{Z}_{\geq 0}$, we have

$$(1 + m)^n \equiv 1 + mn \pmod{m^2}.$$

Solution. The theorem is true for $n = 0$ since $(1 + m)^0 = 1 \equiv 1 + 0n \pmod{m^2}$. Suppose it is true for n; we show it is true for $n + 1$. We have

$$(1 + m)^{n+1} = (1 + m)^n(1 + m) \equiv (1 + mn)(1 + m) = 1 + mn + m + m^2n \equiv 1 + m(n + 1) \pmod{m^2}$$

so the result indeed holds by induction.

Problem 4. Let $n \in \mathbb{Z}_{>4}$. Show that $n \mid (n - 1)!$ if and only if n is composite.

Solution. First, suppose $n = p$ is prime. Then $p \nmid (p - 1)!$, since every prime divisor of $(p - 1)!$ is at most $p - 1$, which is smaller than p.

Now suppose $n = ab$ is composite with $1 < a, b < n$. If $a \neq b$, then since $a, b < n$, each occurs in the product $(n - 1)!$ (which is, after all, the product of all integers from 1 to $n - 1$), so indeed $n \mid (n - 1)!$. If $a = b > 2$, then since $2a < ab = n$, both a and $2a$ occur in the product $(n - 1)!$ so $a^2 = n \mid (n - 1)!$. If $a = b = 2$, then $n = 4$ and then the statement is not true: $4 \nmid 3! = 6$.

Problem 5. Show that $\sqrt{1 + \sqrt{2}}$ is irrational.

Solution. Suppose $a = \sqrt{1 + \sqrt{2}} \in \mathbb{Q}$. Then $1 + \sqrt{2} = a^2 \in \mathbb{Q}$ and $\sqrt{2} = a^2 - 1 \in \mathbb{Q}$. But this is a contradiction, since $\sqrt{2} \notin \mathbb{Q}$: if $\sqrt{2} = p/q$ with $\gcd(p, q) = 1$ then $2q^2 = p^2$ so $2 \mid p$ but then $4 \mid p^2 = 2q^2$ so $2 \mid q$, a contradiction.

Problem 6 (Bonus). A random integer n is chosen between 1 and 10000, inclusive. Approximate the probability that n is odd and composite. *[Hint:* $\log(10) \approx 2.5$.*]*

Solution. The set of odd, composite integers is obtained by taking away the set of even integers and the set of primes, and the intersection between these two sets is only 1 so as an approximation (!) they are disjoint. There are $\pi(10000) = \pi(10^4) \approx 10^4/\log(10^4) \approx 10^4/10 = 1000$ primes and 5000 even integers, so there are about 4000 odd, composite integers up to 10000, and so the probability is about 40%.

In fact, this approximation is pretty good: the exact percentage is 37.72%.