Homework 4 Solutions

Math 55, DIS 101-102

4.1.16 [2 points]

Prove that if $a \equiv b \pmod{m}$ then $a \bmod m = b \bmod m$.

Simplest proof: If $a \equiv b \pmod{m}$ then $m | a - b$, so $a = b + mk$ for some $k \in \mathbb{Z}$. Then if $a = qm + r$ with $0 \leq r < m$, it follows that $b + km = qm + r$ and so $b = (q - k)m + r$. This implies that $a \bmod m = b \bmod m$.

Second proof: Let $a = sm + r_1$ and let $b = tm + r_2$ with $0 \leq r_1, r_2 < m$. If $a \equiv b \pmod{m}$ then $m|(a - b)$, so there exists k such that $km = (sm + r_1) - (tm + r_2)$. So $r_1 - r_2 = (k + t - s)m$, but since $0 \leq r_1, r_2 < m$ the only possibility is $r_1 - r_2 = 0$, which means that $r_1 = r_2$ and $a \bmod m = b \bmod m$.

Many people here jumped directly from saying that $r_1 - r_2 = (k+t-s)m$ to asserting that $r_1 - r_2 = 0$. The intuition is right, but note that it would take a few more lines to prove this step thoroughly. As an example: $r_1 < m$ and $r_2 \geq 0$, so $r_1 - r_2 < m + 0 = m$. But $r_1 \geq 0$ and $r_2 < m$, so $r_1 - r_2 > 0 - m = -m$. The only number divisible by m that satisfies $-m < x < m$ is 0, so $r_1 - r_2 = 0$.

Or a little less formal: We know that $0 \leq r_1, r_2 \leq m - 1$, so if $r_1 \neq r_2$ then their difference is at most $(m - 1) - 0 = m - 1$. But no positive numbers less than m are divisible by m, so $r_1 - r_2$ must be 0.

4.1.37 [2 points] Find counterexamples to the following claims:

1. If $ac \equiv bc \pmod{m}$ and $m \geq 2$ then $a \equiv b \pmod{m}$.
   One way to look at this claim is to rewrite the first condition as $(a - b)c \equiv 0 \pmod{m}$, and the second as $a - b \equiv 0 \pmod{m}$. This suggests $c \equiv 0 \pmod{m}$ as the key to a counterexample, and $a = 1, b = 2, c = m = 3$ suffices.
2. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ with $c, d > 0$ and $m \geq 2$ then $a^c \equiv b^d \pmod{m}$.
   Since exponentiation for integers is just repeated multiplication, we can say that $a^c \pmod{m} = (a \bmod m)^c \pmod{m}$, and similarly for $b^d \pmod{m}$. It follows that if $c = d$ then the claim is true, so to find a counterexample we need to try $c \neq d$.
   Pretty much any random choice will serve as a counterexample: If $a = b = 2$, $c = 1, d = 6$, and $m = 10$, then $2^1 \equiv 2 \pmod{10}$ but $2^6 \equiv 4 \pmod{10}$.

4.2.4 [2 points]

1. Convert $(1010110101)_2$ to decimal.
   $$(1010110101)_2 = 2^0 + 2^2 + 2^4 + 2^5 + 2^7 + 2^9 = 1 + 4 + 16 + 32 + 128 + 512 = 693.$$
2. Convert $(111110000011111)_2$ to decimal.
   Easy way: Notice that $(111110000011111)_2 = (11111)_2 \cdot (10000000001)_2 = 31 \cdot 1025 = 31775$.

4.3.6 [0 points]

How many zeros are there at the end of 100!?

Since $10 = 2 \cdot 5$, the key is to look at the powers of 2 and 5 in 100!. Since the number of fives is the limiting factor, we only need to count the number of fives. There are $\lfloor 100/5 \rfloor = 20$ numbers contributing at least 1 power of five and $\lfloor 100/25 \rfloor = 4$ numbers contributing two powers (25, 50, 75, 100). 100! therefore ends in 24 zeros.

4.3.33 [2 points]

Use the Euclidean algorithm to find

1. $\gcd(1, 5)$: 1, since 1 is the largest divisor of 1.

2. $\gcd(100, 101)$: 1, since consecutive numbers are relatively prime. (Also, 101 is prime.)
3. $\gcd(123, 277)$: 1
4. $\gcd(1529, 14039)$: 139
5. $\gcd(1529, 14038)$: 1, since 1529 and 14039 had a common factor and 14038 and 14039 are consecutive.
6. $\gcd(11111, 111111)$: 1