MATH 51 Homework #13

Tamir Enkhjargal

May 2019

1. Let $a \equiv b \bmod m$ and $b \equiv c \bmod m$. This means that (where $k \in \mathbb{Z}$):

$$a \equiv b \bmod m \rightarrow a - b = mk_1 \tag{1}$$
$$b \equiv c \bmod m \rightarrow b - c = mk_2 \tag{2}$$

$$(1) + (2) = [a - b = mk_1] + [b - c = mk_2] \tag{3}$$
$$= a - c = m(k_1 + k_2) \tag{4}$$

As $k_1 + k_2$ is also an integer, this means that m divides $a - c$, which is the same as $a \equiv c \bmod m$. Therefore the transitie property works $a \equiv b \equiv c \bmod m$ if $a \equiv b$ and $b \equiv c$.

2. Let $a \equiv b \bmod m$ and $c \equiv d \bmod m$. This means that (where $k \in \mathbb{Z}$):

$$a \equiv b \bmod m \rightarrow a - b = mk_1 \tag{1}$$
$$c \equiv d \bmod m \rightarrow c - d = mk_2 \tag{2}$$
$$ac \equiv bd \bmod m \rightarrow ac - bd = mk_3 \tag{3}$$
$$= a(c - d) + (a - b)d = mk_3 \tag{4}$$
$$= a(mk_2) + (mk_1)d = mk_3 \tag{5}$$
$$= m(ak_2 + k_1 d) = mk_3 \tag{6}$$

Since $ak_2 + k_1 d$ is $\in \mathbb{Z}$, this shows that $ac \equiv bd \bmod m$

3.

n	$n^2 + n + 1$	$n^2 + n + 1 \bmod 3$
1	3	0
2	7	1
3	13	1
4	21	0
5	31	1
6	43	1
7	57	0
...	...	...

m	$3m + 2$	$3m + 2 \bmod 3$
1	5	2
2	8	2
3	11	2
4	14	2
5	17	2
6	20	2
...	...	...

Since the results of $n^2 + n + 1 \equiv (0, 1) \bmod 3$ and $3m + 2 \equiv 2 \bmod 3$, we showed that $n^2 + n + 1 \not\equiv 3m + 2 \bmod 3$

4. Prove that if n is an odd positive integer, then $n^2 \equiv 1 \bmod 8$.

   We can look at all of the possible results of $n \bmod 8$:

n	$n \bmod 8$
1	1
3	3
5	5
7	7
9	1
11	3
13	5
...	...

   All reduced $n \in \{1, 3, 5, 7\} \bmod 8$. Because multiplication is respected in mod, we can square then mod, or mod then square. We will now square the only possible reductions:

n	n^2	$n^2 \bmod 8$
1	1	1
3	9	1
5	25	1
7	49	1

   Therefore, $n^2 \equiv 1 \bmod 8$ for all positive odd integers n.

5.

$$
\begin{aligned}
(p \vee q) \to r &\equiv (p * q + p + q) \to r && (1)\\
&\equiv (p * q + p + q)r + (p * q + p + q) + 1 && (2)\\
&\equiv p * q * r + p * r + q * r + p * q + p + q + 1 && (3)
\end{aligned}
$$

$$
\begin{aligned}
(p \to r) \wedge (q \to r) &\equiv (p * r + p + 1) \wedge (q * r + q + 1) && (4)\\
&\equiv (p * r + p + 1) * (q * r + q + 1) && (5)\\
&\equiv p * q * r^2 + 2 * p * q * r + p * r + q * r + p * q + p + q + 1 && (6)\\
&\equiv p * q * r + p * r + q * r + p * q + p + q + 1 && (7)
\end{aligned}
$$

From both sides, we converted to a Boolean expression, and arrived at the same equivalency.