## MATH 8: ASSIGNMENT 25

## APRIL 28, 2019

## Summary of previous

Recall that we say that $t$ is inverse of $a \bmod n$ if $a t \equiv 1 \bmod n$.
Theorem. A number a has an inverse mod $n$ if and only if a is relatively prime with $n$, i.e. $\operatorname{gcd}(a, n)=1$.
If $a$ has an inverse $\bmod n$, then we can easily solve equations of the form

$$
a x \equiv b \quad \bmod n
$$

Namely, just multiply both sides by inverse of $a$.

## Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem). Let $a, b$ be relatively prime. Then the following system of congruences:

$$
\begin{array}{lc}
x \equiv k & \bmod a \\
x \equiv l & \bmod b
\end{array}
$$

has a unique solution mod ab, i.e. there exists exactly one integer $x$ such that $0 \leq x<a b$ and $x$ satisfies both the above congruences.

Proof. Let $x=k+t a$ for some integer $t$. Then $x$ satisfies the first congruence, and our goal will be to find $t$ such that $x$ satisfies the second congruence.

To do this, write $k+t a \equiv l \bmod b$, which gives $t a \equiv l-k \bmod b$. Notice now that because $a, b$ are relatively prime, $a$ has an inverse $h \bmod b$ such that $a h \equiv 1 \bmod b$. Therefore $t \equiv h(l-k) \bmod b$, and $x=k+a h(l-k)$ is a solution to both the congruences.

To see uniqueness, suppose $x$ and $x^{\prime}$ are both solutions to both congruences such that $0 \leq x, x^{\prime}<a b$. Then we have

$$
\begin{gathered}
x-x^{\prime} \equiv k-k \equiv 0 \quad \bmod a \\
x-x^{\prime} \equiv l-l \equiv 0 \quad \bmod b
\end{gathered}
$$

Thus $x-x^{\prime}$ is a multiple of both $a$ and $b$; because $a, b$ are relatively prime, this implies that $x-x^{\prime}$ is a multiple of $a b$, but if this is the case then $x$ and $x^{\prime}$ cannot both be positive and less than $a b$ unless they are in fact equal.

## Homework

1. Is it possible for a multiple of 3 to be congruent to $5 \bmod 12$ ?
2. (a) Find inverse of $7 \bmod 11$.
(b) Find all solutions of the equation

$$
7 x \equiv 5 \quad \bmod 11
$$

3. Solve the following systems of congruences
(a)

$$
\begin{array}{ll}
x \equiv 1 & \bmod 3 \\
x \equiv 1 & \bmod 5
\end{array}
$$

(b)

$$
\begin{array}{ll}
z \equiv 1 & \bmod 5 \\
z \equiv 6 & \bmod 7
\end{array}
$$

4. (a) Find the remainder upon division of $23^{2019}$ by 7 .
(b) Find the remainder upon division of $23^{2019}$ by 70. [Hint: use $70=7 \cdot 10$ and Chinese Remainder Theorem.]
5. (a) Find the remainder upon division of $24^{46}$ by 100 .
(b) Determine all integers $k$ such that $10^{k}-1$ is divisible by 99 .
6. In a calendar of some ancient race, the year consists of 12 months, each 30 days long. They also use 7 day weeks, same as we do.

If first day of the year was a Monday, will it ever happen that 13th day of some month is a Friday? If so, when will be the first time it happens, and how often will it repeat afterwards?
[Hint: this can be rewritten as a system of congruences: $n \equiv 5 \bmod 7, n \equiv 13 \bmod 30$.]
7. How many remainders mod 2310 can be expressed as powers of 6 ?

