## Worksheet 11: Wilson's Theorem, Chinese Remainder Theorem, Review

**Problem 1.** Pair off the numbers $1, 2, \ldots, 16$ into pairs of inverses mod 17. *Note*. Two of these numbers don't really make "pairs"...

**Problem 2.** Find the remainder when 15! is divided by 17.

*Solution.* By Wilson's theorem, we know that $16! \equiv -1 \bmod 17$. This means that $15! \equiv -16^{-1} \equiv (-1)^{-1} \bmod 17$. But clearly $(-1)^{-1} \equiv -1$, so $15! \equiv 1 \bmod 17$.

**Problem 3.** Find an integer having remainders 1, 2, 5, 5, when divided by 2, 3, 6, 12, respectively. *Note*. This problem is attributed to 6th century mathematician Yī Xíng.

**Problem 4.** When eggs in a basket are removed 2, 3, 4, 5, 6 at a time, there remain 1, 2, 3, 4, 5 eggs, respectively. When they are taken out 7 at a time, none are left over. Find the smallest number of eggs that could have been in the basket. *Note*. This problem is attributed to 7th century mathematician Brahmagupta.

**Problem 5.** Find an integer having remainders 3, 11, 15 when divided by 10, 13, 17, respectively. *Note*. This problem is attributed to 15th century mathematician Regiomontanus.

**Problem 6.** Find three consecutive integrs, each having a square factor.

*Solution.* We can use the Chinese Remainder Theorem to find a solution to the following system

$$\begin{aligned} x &\equiv 0 \bmod 2^2 \\ x+1 &\equiv 0 \bmod 3^2 \\ x+2 &\equiv 0 \bmod 5^2 \end{aligned}$$

Calculation omitted. One can also compute this in Sage using `CRT_list([0,-1,-2], [4,9,25])`. The solution is 5468. Thus the three consecutive integers are 5468, 5469, 5470.

**Problem 7.** Find the smallest positive integer $a$ such that $2 \mid a, 3 \mid a+1, 4 \mid a+2, 5 \mid a+3$ and $6 \mid a+4$.

**Problem 8.** Without using a calculator or computer, find the last two digits of $1032^{1032}$. *Hint*. Find the remainders modulo 4 and 25, and then use the Chinese Remainder Theorem to find the remainder modulo 100.

*Solution.* Observe that $1032 \equiv 0 \bmod 4$, so $1032^{1032} \equiv 0^{1032} = 0 \bmod 4$. Also, we have $1032 \equiv 7 \bmod 25$. Since $\varphi(25) = 5 \cdot 4 = 20$, Euler's theorem tells us that $7^{20} \equiv 1 \bmod 25$. Now $1032 = 20q + 12$ for some integer $q$, so

$$7^{1032} = (7^{20})^q 7^{12} \equiv 7^{12} \bmod 25.$$

Note that $7^2 \equiv 49 \equiv -1 \bmod 25$, so $7^{12} = (7^2)^6 \equiv (-1)^6 \equiv 1 \bmod 25$. Thus $1032^{1032}$ is a solution to the following system.

$$\begin{aligned} x &\equiv 0 \bmod 4 \\ x &\equiv 1 \bmod 25 \end{aligned}$$

On the other hand, we can also calculate a solution to this system using the Chinese Remainder Theorem. We can eyeball Bézout coefficients

$$1 = (-6) \cdot 4 + 1 \cdot 25$$

so $x = 0 + 1 \cdot (-6) \cdot 4 = -24 \equiv 76 \bmod 100$ is the unique solution to the system. Thus $1032^{1032} \equiv 76 \bmod 100$, ie, the last two digits are 100.

**Problem 9.** Show that there exist infinitely many primes $p$ such that $p+2$ is *not* prime. *Remark*. If you remove the word "not" from this statement, you would obtain the statement of the twin prime conjecture, which is a famous unsolved problem in number theory!

*Solution.* Let's say that $S$ is the set of all primes such that $p+2$ is not prime, and suppose for a contradiction that $S$ is finite. Let $p_0$ be a prime that's bigger than all of the primes in $S$. We know that such a prime exists by Euclid's theorem on the infinitude of primes. Moreover, note that $2 \in S$, so it must be that $p_0 > 2$. In particular, $p_0$ is odd.

We claim that every odd integer greater than $p_0$ must be prime. In other words, we claim that $p_0 + 2r$ is prime for every integer $r \geqslant 0$. Let us prove this by induction. The base case $r = 0$ is true by our choice of $p_0$. Suppose it is true

for some $r = k$. Then $p_0 + 2(r+1) = (p_0 + 2r) + 2$. We know that $p_0 + 2r$ is prime by our inductive hypothesis, and it is not in $S$ since $p_0 + 2r \geqslant p_0$ and $p_0$ is greater than all of the elements of $S$. But $p_0 + 2r$ being prime while $p_0 + 2r \notin S$ means precisely that $(p_0 + 2r) + r = p_0 + 2(r+1)$ is prime. This completes the induction.

Now suppose $n$ and $m$ are two odd numbers bigger than $p_0$. Then $nm$ is also odd and bigger than $p_0$, but it is not prime since $n$ and $m$ are nontrivial factors. This contradicts our observation above that every odd number bigger than $p_0$ is prime.

**Problem 10.** The cells in a jail are numbered from 1 to 100 and their doors are activated from a central button. Activation opens a closed door and closes an open door. The $k$th time the button is pressed, all doors that are multiples of $k$ are activated. If all doors are initially closed and the button is pressed 100 times, which doors will be open at the end? *Suggestion*. Try going through this process by hand with 20 instead of 100 first to get a feeling for the problem.

*Solution.* In order for a given door $n$ to be open at the end, it needs to be activated an odd number of times. It'll be activated on the $k$th press for every $k$ that divides $n$, so we need for $n$ to have an odd number of divisors. If $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of $n$, the possible divisors of $n$ are $k = p_1^{f_1} \cdots p_r^{f_r}$ where $0 \leqslant f_i \leqslant e_i$. In other words, there are $e_i + 1$ choices for each $f_i$, so the total number of divisors of $n$ is

$$(e_1 + 1) \cdots (e_r + 1).$$

In order for this to be odd, we need for each $e_i + 1$ to be odd, which means we need each $e_i$ to be even. In other words, $n$ needs to be a perfect square. The perfect squares less than or equal to 100 are 1, 4, 9, 16, 25, 36, 49, 81, and 100.