Putnam Problem-Solving Seminar Week 4
Modular Arithmetic, Continued

There are too many problems to consider each one in one session alone. Just pick a few problems that you like and try to solve them. However, you are not allowed to work on a problem that you already know how to solve.

Hints. Work in groups. Try small cases. Do examples. Look for patterns. Use lots of paper. Talk it over. Choose effective notation. Try the problem with different numbers. Work backwards. Argue by contradiction. Eat pizza. Modify the problem. Generalize. Don't give up after five minutes. Don't be afraid of a little algebra.

Modular Arithmetic Definitions and Facts.

- $x \equiv y \pmod{n}$ if x and y both give the same remainder upon division by n
- Equivalently, $x \equiv y \pmod{n}$ if $x-y$ is divisible by n, i.e. $x-y \equiv 0 \pmod{n}$
- $\varphi(n)$ is equal to the number of integers a such that $1 \leq a \leq n$ and $gcd(a,n) = 1$
- If $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, then $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\dots(1-\frac{1}{p_r})$
- Euler's Theorem: If $gcd(a,n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$
- Fermat's Little Theorem: If p is a prime, then $a^{p-1} \equiv 1 \pmod{p}$

Problems.

1. Determine 51 mod 13, 342 mod 85, 62 mod 15, 10 mod 15, $(82 \cdot 73)$ mod 7, $(51+68)$ mod 7, $(35 \cdot 24)$ mod 11, and $(47+68)$ mod 11.
2. A USPS money order has an identification number consisting of 10 digits together with an extra digit called a *check*. The check

digit is the 10-digit number modulo 9. For example, the number 3953988164 has the check digit 2 since 3953988164$\equiv$ 2 mod 9. If the number 39539881642 were entered incorrectly into a computer as, say 39559881642, the machine would calculate the check as 4, whereas the entered check digit would be 2, so the error would be detected. Determine the check digit for the number 07312400508.

3. Compute 5^{15} modulo 7 and 7^{13} modulo 11.
4. Prove that 3, 5, and 7 are the only three consecutive odd integers that are prime.
5. Find the last digit of 7^{100}.
6. Show that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3.
7. Show that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.
8. Show that $(d_k d_{k-1} \dots d_1 d_0)$ is divisible by 11 if and only if $d_k - d_{k-1} + d_{k-2} - \dots \pm d_0$ is divisible by 11.
9. Show that $x^2 - 1 \equiv 0 \pmod 8$ has four solutions.
10. Let p be a prime number. Show that $x^2 \equiv 1 \pmod p$ if and only if $x \equiv \pm 1 \pmod p$.
11. Let q be a prime factor of $a^2 + b^2$. Show that if $q \equiv 3 \pmod 4$, then $q|a$ and $q|b$.
12. Find the least positive integer x such that $13|(x^2 + 1)$.
13. Prove that any number that is a square must have one of the following for its units digit: 0, 1, 4, 5, 6, 9
14. Prove that 19 is not a divisor of $4n^2 + 4$ for any integer n.
15. Show that $7|(3^{2n+1} + 2^{2n+2})$ for all n.
16. Prove that $n^6 - 1$ is divisible by 7 if $gcd(n, 7) = 1$.

17. Prove Wilson's Theorem: If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

18. Prove that $n^7 - n$ is divisible by 42 for any integer n.

19. Prove that $n^{13} - n$ is divisible by 2, 3, 5, 7, and 13 for any integer n.

20. Prove that the product of three consecutive integers is divisible by 504 if the middle one is a cube.

21. What is the last digit of 3^{400}?

22. Show that an integer $m > 1$ is prime if and only if m divides $(m-1)! + 1$.

23. For what values of n is $\varphi(n)$ odd?

24. Show that $\varphi(nm) = n\varphi(m)$ if every prime that divides n also divides m.

25. Characterize the set of positive integers n satisfying $\varphi(2n) = \varphi(n)$.

26. Find all solutions x of $\varphi(x) = 24$.

27. Prove that there are infinitely many integers n such that 3 does not divide $\varphi(n)$.