Number Theory

Instructor: Dušan Djukić

Problems – April 21

1. Define $a_n = 2^n + 3^n + 6^n - 1$ for each positive integer n. Find all primes that do not divide any term of this sequence.

2. If a and b are any coprime positive integers, prove that there are infinitely many exponents n for which $a^n + b$ is composite.

3. Prove that there is an infinite set of pairwise coprime integers of the form $2^n - 3$.

4. Define $a_1 = 2$ and $a_{n+1} = 2^{a_n} + 2$ for all n. Prove that a_m divides a_n whenever $m < n$.

5. If a is odd and $k \geqslant 3$, prove that $a^{2^{k-2}} \equiv 1 \pmod{2^k}$.

- Define $\lambda(p^k) = p^{k-1}(k-1)$ for any odd prime p and $k \geqslant 1$.
  Also define $\lambda(2^k) = 2^{k-2}$ for $k \geqslant 2$, with $\lambda(2) = 1$ and $\lambda(4) = 2$.
  Finally, define $\lambda(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \operatorname{lcm}[\lambda(p_1^{\alpha_1}), \dots, \lambda(p_k^{\alpha_k})]$.

  Then $a^{\lambda(n)} \equiv 1 \pmod{n}$ whenever a is coprime to n. *(Carmichael's theorem)*

- Given coprime integers a, n with $|a| > 1$ and $n \neq 0$, the *multiplicative order* of a modulo n is the smallest r such that $a^r \equiv 1 \pmod{n}$.

  The order modulo n always divides $\varphi(n)$.

6. Find the order of 3 modulo 2021.

7. (a) If p is an odd prime divisor of $x^2 + 1$, prove that $p \equiv 1 \pmod{4}$.

   Does this remain valid if p needn't be prime?

   (b) If a prime p divides $x^2 + y^2$ and $p \equiv 3 \pmod{4}$, prove that p divides both x and y.

8. Prove that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

9. Let $p > 2$ be a prime. Prove that every divisor of $2^p - 1$ is congruent to 1 modulo $2p$.

10. Prove that there are infinitely many primes of the form $2px + 1$. But don't use Dirichlet's theorem.

11. Let p be a prime and let n be coprime to $p-1$. Prove that th numbers $1^n, 2^n, \dots, (p-1)^n$ are all distinct modulo p.