Name: **Student ID:**

Sample Test II.

The actual test will have 5 questions and perhaps one bonus question. You will have 50 minutes to answer them, without using your notes or communicating with other students. You will have to give the simplest possible answer and show all your work.

1. Using the Chinese Remainder Theorem, solve the system of congruences

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 5 \pmod{6} \\ 2x &\equiv 7 \pmod{5} \end{aligned}$$

2. State and outline the proof of Fermat's little theorem.

3. State and outline the proof of Wilson's theorem.

4. Let p be an odd prime. Using Wilson's theorem, prove that

$$(p-2)! \equiv 1 \pmod{p}.$$

5. If f is a multiplicative function and F is defined by $F(n) = \sum_{d|n} f(d)$, then F is multiplicative. Prove this claim.

6. Let $\tau(n)$ be the number of divisors of n, and $\mu(n)$ the Möbius function. Prove that

$$\sum_{d|n} \mu(d)\tau\left(\frac{n}{d}\right) = 1.$$

7. Let $\sigma(n)$ the sum of divisors of n and $\mu(n)$ the Möbius function. Prove that

$$\sum_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right) = n.$$

8. Explain why σ and τ are multiplicative functions.

9. Determine the exponent of the highest power of 7 appearing in the prime factorization of 140!.

10. Prove the formula

$$\sum_{d|n} \phi(d) = n.$$

11. Is the Euler function ϕ multiplicative? Justify your answer!

12. Calculate $\phi(1234)$.

13. Prove that the product of two multiplicative functions is multiplicative (We define the product $f \cdot g$ by $(f \cdot g)(n) := f(n) \cdot g(n)$.)

14. Which powers of $\rho = \cos(\frac{2\pi}{30}) + i\sin(\frac{2\pi}{30})$ are primitive thirtieth (complex) roots of unity? Give a formula for the number of primitive n-th complex roots of unity. Justify the formula.

15. Prove that for a prime number p and a divisor d of $p-1$, the congruence

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d solutions.

16. State for which values of n is there a primitive root of n.

17. What is the number of primitive roots for n (provided there is at least one)?

18. For which powers of 2 is there a primitive root? Justify your answer by providing a primitive root when it exists, and a proof of non-existence to cover the remaining cases.

19. Assume that $m > 2$ and $n > 2$ are relative primes. Prove that $m \cdot n$ has no primitive root.

20. Assuming that r is a primitive root of the odd prime p, how would you find a primitive root of p^2?

B **Bonus question:** State and outline the proof of Euler's generalization of Fermat's little theorem.

Good luck. Gábor Hetyei