

Basics

Problem 1. Calculate $1 + 4 + 7 + 7 + 13 + 16 + 19 + 19 + \cdots + 991 + 991 + 997 + 1000$

Problem 2. Calculate $\gcd(2101, 1009)$ using Euclid's Algorithm. Show your steps clearly.

Problem 3. Find the multiplicative inverse of 12345 modulo 211.

Problem 4. Given bankrate $b = 1.05$, calculate the value after 5 years if someone deposits \$1,000 at the beginning of the first year.

Problem 5. Given bankrate $b = 1.10$, how much should you deposit at the beginning of the first year so that you can get \$100,000 after 10 years?

Problem 6. Solve the followings, or give "unsolvable" if it has no solution.

(a) $19x \equiv 20 \pmod{77}$

(b) $49x \equiv 98 \pmod{21}$

(c) $105x \equiv 143 \pmod{100}$

Medium

Problem 1. Calculate $987^{65} \pmod{17}$ by repeated squaring.

Problem 2. Prove that any positive integer N is divisible by 6 if and only if N is even and divisible by 3.

Problem 3. Let $f(a, b) = \frac{a!}{(a-b)!b!}$. Find the remainder when $f(100, 3)$ is divided by 7.

Problem 4. Prove that if p is prime and $p|ab$, then $p|a$ or $p|b$.

Problem 5. Let x be a positive integer. Find all x such that $x^{2110} \equiv 2 \pmod{5}$.

Problem 6. Under RSA, given $p = 31, q = 19, n = pq, T = (p-1)(q-1)$.

(a) Let $e = 101$, calculate d such that $e \times d \equiv 1 \pmod{T}$ using extended Euclid's algorithm.

(b) Encrypt the message $m = 777$ into m' . You may use repeated squaring to speed up the calculations.

(c) Decrypt m' to get m again. You may use repeated squaring to speed up the calculations.

Problem 7. Solve the smallest x that satisfies the followings:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv 4 \pmod{7}$$

$$x \geq 100$$

Problem 8. Prove the followings:

- (a) For n_i 's being relatively prime, $n_i|x$ for $i = 1, 2, \dots, k$ implies $n_1 n_2 \cdots n_k | x$.
- (b) Hence, prove the uniqueness of the Chinese remainder theorem of the solution modulo $n_1 n_2 \cdots n_k$.

Problem 9. Show how to get 99 gallons of water by using 243 and 342 gallon jugs. Please reduce number of rounds of transferring water.

Problem 10. Show that $m^{13} - m$ is divisible by 13.

Problem 11. We are going to study *strong primality test*.

- (a) Show that, using strong primality test, 91 is prime by using 22, 29, 38 as bases.
- (b) Can you conclude that 91 is prime by testing these three bases? If not, please find another base and use strong primality test to show that it is composite.

Problem 12. The Indian mathematician Brahmagupta, born in A.D. 598, posed the following problem: There are n eggs in a basket. When eggs are removed 2, 3, 4, 5, or 6 at a time, the number left over is 1, 2, 3, 4, or 5, respectively. Only when eggs are removed at 7 at a time is none left over. What is the least number of eggs that could be in the basket?

Problem 13. John loves buying antique and sells it out someday. He loves so because he believes that it will give him more wealth. But John wants to maximize his profit by any mean. Given an antique that costs \$2,000,000, and it inflates 6%, the bankrate is 12%, loan period is 20 years, payments and rates are considered annually. John has two plans:

- (a) He borrows \$2,000,000 to buy the antique.
- (b) Instead of buying the antique, John would use the annual payment to do investment in the stock market. Suppose it gives 12% annual return.

Which plan will John choose if he wants to maximize his wealth after 20 years?

Problem 14. Denote a function f such that for any positive real numbers x, y, z ,

$$f(x, y, z) = \frac{x}{y} + \sqrt{\frac{y}{z}} + \sqrt[3]{\frac{z}{x}}$$

Prove that $f(x, y, z) \geq \sqrt[3]{4} \times \sqrt{3}$. Also state that when will the equality hold.

Hard

Problem 1. Remember **Q2(c)** of homework 1? We proved that product of two sum of squares is also sum of squares. We wish to extend more from this proof. Before that, denote \mathbb{P} as the set of prime numbers and \mathbb{S} as the set of numbers that are sum of squares.

- (a) Prove that if $u, v \in \mathbb{S}$ and $v \in \mathbb{P}$ so that $v|u$, then $\frac{u}{v} \in \mathbb{S}$. (*Hint: Construct $xu - yv$ so that we can factorize this term.*)
- (b) Hence, or otherwise, prove that if $w \notin \mathbb{S}$ and $u \in \mathbb{S}$ so that $w|u$, there exists z so that $z|\frac{u}{w}$ and $z \notin \mathbb{S}$.
- (c) Prove that if $\gcd(u, v) = 1$, then for all integers s such that $s|(u^2 + v^2)$, $s \in \mathbb{S}$.
- (d) Hence, or otherwise, prove that for any integer that can be written as $4m + 1 \in \mathbb{P}$, $4m + 1 \in \mathbb{S}$.

Problem 2. Prove that for $n = 1, 2, \dots$, we have

$$2\sqrt{n+1} - 2 < 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \dots + \frac{1}{\sqrt{n}} \leq 2\sqrt{n} - 1$$

Problem 3. Let H_n be such that $H_n = \sum_{i=1}^n \frac{1}{i}$.

- (a) Prove the inequalities $\ln n < H_n \leq \ln n + 1$ by induction on n . You may use the fact that for any real number x , we have $1 + x \leq e^x$
- (b) Solve (a) using integrals.

Problem 4. You plan to send a truck to carry n tanks of gas over a desert. With 1 tank (each contains 1 unit of gas), the truck can only go 1 unit distance. You decide such strategy: On the starting point, you plan to carry 1 tank with a truck x unit far, putting $1 - 2x$ unit of gas there, and using the remaining x unit of gas back to the starting point. When you carry the last tank, you just put $1 - x$ unit of gas there since you won't go back to the starting point again. Instead, you will let that new position as the starting point and repeat the same process. Prove that you can cross any desert by choosing suitable n .