Modular Arithmetic

Warm-ups

Try these problems to get used to modular arithmetic!

1. Reducing: What is $5 \mod 3$? How about $124209 \mod 10$? What about $3970491 \mod 9$? Can you find a rule for reducing modulo 9?

2. Addition: What is $3 + 8 \mod 3$? What about $3 - 17 \mod 6$?

3. Multiplication: What is $4 \cdot 5 \mod 6$? What is $3 \cdot 2 \mod 5$? What about $19 \cdot 21 \mod 5$?

Strange properties

There are some unusual things that happen in modular arithmetic.

4. Zero and one: In modulo 6, which numbers multiply to equal 1 (we call these numbers units)? Which numbers multiply to equal 0? Can you answer these questions for any modulus? Try some other examples to get started.

5. Division: Can we divide numbers in modular arithmetic? If so what should $\frac{1}{4}$ be in modulus 5. (remember, the only elements in modulus 5 are 0,1,2,3 and 4). Can you find a number that is $\frac{1}{4}$ in modulus 6? In general which numbers can we divide by?

6. Exponents: What is $2^5 \mod 3$? Can you find $3^{102} \mod 7$? What is the last digit of 3^{2017}?

Formalizing some rules

Let's practice writing sum proofs of arithmetic rules.

7. Prove that $a + b \mod n = (a \mod n) + (b \mod n)$.

8. Write and prove a similar statement for multiplication.

9. Write and prove a statement about exponentiation in modular arithmetic.

Addition and multiplication tables

Make a multiplication table for modulus 2, modulus 3, modulus 4, modulus 5 and modulus 7. Do notice anything or see any patterns?

Divisors of n

We say n and m are coprime if they share no prime factors.

10. How can you tell if m and n are coprime? Are 9143 and 2701 coprime?

11. How many divisors does p have? How many divisors does p^2 have? How many divisors does a general number n have?

12. How many elements of modulus n are units (multiply with another number to equal 1)?

Amazing proofs

These facts are both surprising and useful.

13. Prove that $(x+y)^p = x^p + y^p \mod p$ where p is prime and x and y are variables.

14. Prove that $a^p = a \mod p$.

15. Prove that if $a = b \mod p-1$ then $c^a = c^b \mod p$.

More things to try

If you finish everything else, think about these problems. Some are easier than others and they might involve ideas outside the scope of this worksheet.

16. What integers have a square root modulo p? How many of them are there?

17. Simplify $\binom{a \cdot p}{b \cdot p} \mod p$.

18. A perfect number is a number that equals the sum of its divisors. Show that if a is an odd perfect number, then $a = 1 \mod 4$.

19. Multiplying 10112359550561797752808988764044943820224719 by 9 moves the 9 at the end to the front. Are there any other numbers that have this property?

20. Let F_n denote the nth Fibonacci number and let p be an odd prime. Show that if 5 has a square root mod p then F_{p-1} is divisible by p.