Discrete Structures

Worksheet 6

Spring 2021
February 10/12

1. **Warm up:** Explain in your own words (not using textbook definitions) what the following expressions mean. All variables are integers.

   (a) $a \mid b$

   (b) $c \equiv d \pmod{e}$

   (c) $\lfloor \frac{f}{2} \rfloor$

   (d) $(g_1 g_2 g_3 g_4 g_5)_g$

   (e) $\gcd(h, k) = \ell$

   (f) $\operatorname{lcm}(m, n) = p$

2. Let $a, b, c \in \mathbf{Z}$.

   (a) Prove that if $a \mid b$ and $c \mid d$, then $ac \mid bd$.

   (b) If $c \neq 0$, prove that $ac \mid bc$ if and only if $a \mid b$.

3. Let n and k be positive integers.

   (a) Express $\lceil \frac{n}{k} \rceil = a$ and $\lfloor \frac{n}{k} \rfloor = b$ as statements without the ceiling and floor symbols, and beginning with "There exists...".

   (b) Prove that $\lceil \frac{n}{k} \rceil = \lfloor \frac{n-1}{k} \rfloor + 1$.

4. Let $n \in \mathbf{N}$.

   (a) Prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

   (b) If $n \geqslant 2$, prove that $n^4 + n^2 + 1$ is composite.

5. Let $a, b \in \mathbf{Z}$.

   (a) What is the relationship between the gcd of a, b and the lcm of a, b? Express it as an equation.

   (b) If $c \in \mathbf{N}$, prove that $\gcd(ac, bc) = c \cdot \gcd(a, b)$.

6. Let $m, n \in \mathbf{N}$ with $m \leqslant n$. Prove that $\dfrac{\gcd(m, n)}{n} \dbinom{n}{m}$ is an integer.

7. Complete the rows in the table below by converting numbers to different bases.

base 2	base 8	base 10	base 16
1010101			
	767676		
		90909	
			AF6446FA

8. Trace out $x, power, i$ in the fast modular exponentiation algorithm (Algorithm 5 on page 268) on the inputs $b = 7$, $m = 11$, and $n = 77$.

9. Trace out x, y, r in the Euclidean algorithm (Algorithm 1 on page 284) on the inputs $a = 31463$ and $b = 9782$.

10. A 12 digit number is named a *valid UPC* (Universal Product Code) iff the digits satisfy the congruence:

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{12}.$$

Replace the digit `X` in the following number to make it a valid UPC: `780194 55330X`.

11. A 13 digit number with digits $a_1 a_2 \ldots a_{13}$ is named a valid 13-digit ISBN (International Standard Book Number) if it satisfies the following congruence:

$$\sum_{k=1}^{7} a_{2k-1} + 3 \cdot \sum_{k=1}^{6} a_{2k} \equiv 0 \pmod{10}.$$

(a) Replace the digit `X` in the following number to make it a valid ISBN: `97809815316X9`.

(b) Does the number correspond to a real book?

12. The Website `https://www.darkcoding.net/credit-card-numbers/` contains some fake credit-card numbers used for testing. Pick any two 16-digit numbers (one MasterCard look=alike number starting by "5"; another Visa look-alike number starting by "4") and check, if they satisfy the Luhn check. (Algorithm for the Luhn check can be looked up in the Wikipedia article.)
Is it possible that somebody accidentally changes one digit in a Credit Card Number to another digit (or swaps two different digits next to each other) – and the resulting number still satisfies the Luhn check?

13. Is it possible to prove (just with a hand calculation and without computing equipment) that the number $2^{99} + 1$ is not a prime?
Hint. You can use algebraic identities to factorize $a^{2n+1} + b^{2n+1}$ to find a number it is divisible by.

14. Use the following Python expressions to find, if $r = 2$, $r = 3$, $r = 7$ are *primitive roots* modulo 19 (namely, if the sequence r^k $(k = 1, \ldots, 16)$ contains all possible non-zero congruence classes (mod 19):

```
list(map(lambda x: 2**x % 19, range(1,19)))
set(map(lambda x: 2**x % 19, range(1,19)))

list(map(lambda x: 3**x % 19, range(1,19)))
set(map(lambda x: 3**x % 19, range(1,19)))
```

15. Using $r = 3$ as a primitive root, write all its powers in the 18 circles in Figure 1. Answer the following questions (referring to the figuresd, if necessary).

(a) What is the inverse number of number 7 modulo 19 (number $\overline{7}$ with the property:

$$\overline{7} \cdot 7 \equiv 1 \pmod{19}.$$

(b) For what remainders a is it possible to solve the quadratic equation:

$$x^2 \equiv a \pmod{19}.$$

(c) Find the discrete logarithm $\mathrm{ind}_3 a \pmod{19}$ (solve the exponential congruences):

$$3^x \equiv a \pmod{19},$$

for $a = 1, 2, 3, 4, 5$.

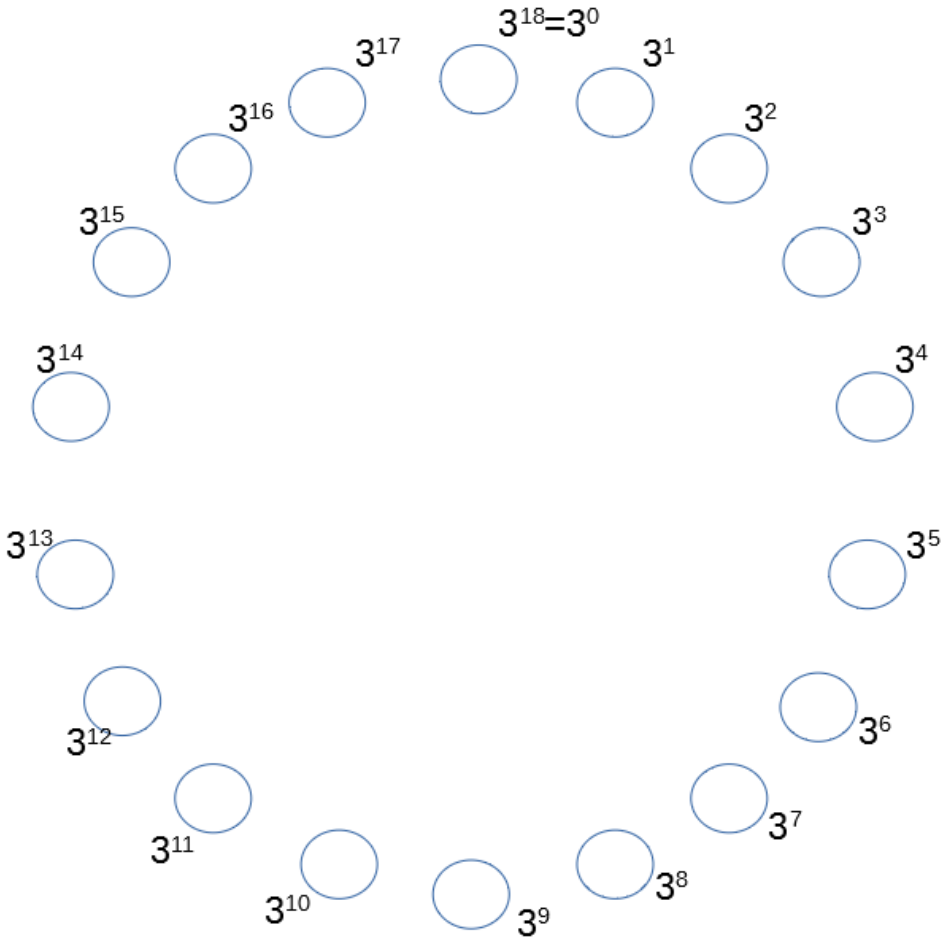

Figure 1: The powers of primitive root $r = 3$ modulo 19.

16. Use M.Knepley textbook (pp.140–151, Chapter 5.3.1 in `https://bit.ly/2MRVJkz`) to find the Coq-proofs for some statements about integer divisiblity:

```
Lemma divide_refl : forall n, (n | n).
Lemma divide_trans : forall n m p, (n | m) -> (m | p) -> (n | p).
Lemma divide_antisymmetric : forall m n : Z, (m > 0) -> (n > 0) ->
            (m | n) -> (n | m) -> (m = n).
Lemma div_ring : forall m n d x y : Z, (d | x) /\ (d | y) ->
            (d | m*x + n*y).
```

Pay attention to some new proof tactics used there: `rewrite` (replace a subexpression from some hypothesis in another hypothesis or in the goal), `unfold Z.divide` (show the meaning of the "divide" symbol, the vertical bar), `ring` (simplify both sides of the expression using ring axioms).