DISCRETE MATH 37181 HOMEWORK SHEET 9

Instructions. Try these sometime after your tutorial and before the next lecture. Set aside some time each week to keep up with the homework. Partial solutions at the end of the PDF.

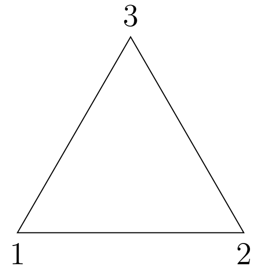
1. Compute the multiplicative inverse mod 216 of 5. [1]

2. Compute $\phi(2223)$. [2]

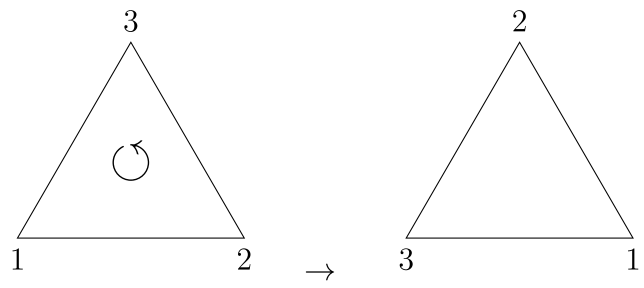
3. Let $a, b, n \in \mathbb{Z}$ and suppose that a and n are relatively prime. Prove that if $n \mid ab$ then $n \mid b$.

4. Let $a, b, c, d, n \in \mathbb{Z}$ and suppose that a and n are relatively prime. Prove that $ab \equiv ac \mod n$ implies $b \equiv c \mod n$.

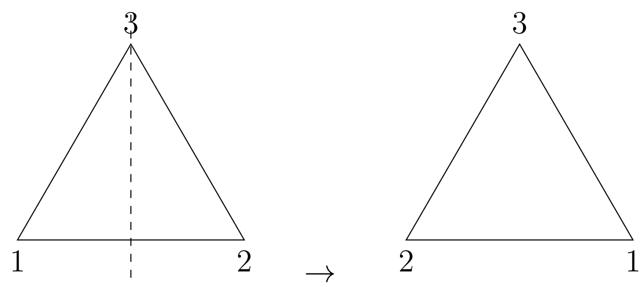
5. Recall Question 7 from Tutorial Worksheet 9, where the concept of a *group* is defined. Consider a triangle with corners labeled $1, 2, 3$.



Let G be the set of all possible ways you can pick up the triangle, move it in 3-D space, then put it back down so that it sits in the same place (but the corners can be in different positions). For example, if we rotate the triangle anti-clockwise $\frac{2\pi}{3}$ radians, we get



and if we instead flip the triangle through a vertical line passing through the centre of the triangle we get

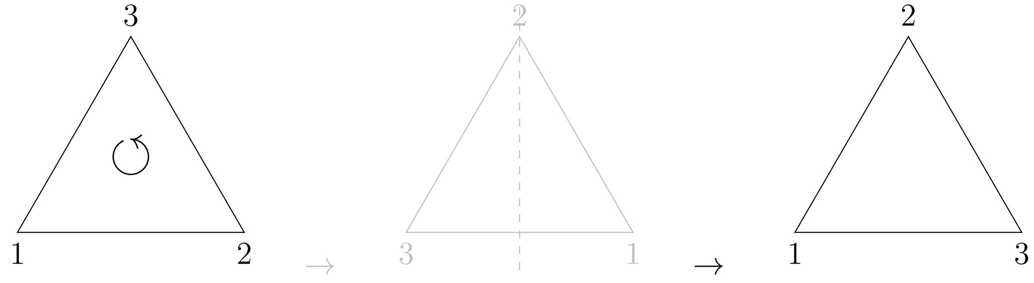


Date: Week 9.

[1] that is, find d so that $5d \equiv 1 \mod 216$. Hint: Euclidean algorithm, then run it backwards.

[2] Hint: Find a prime factorisation of 2223, then use the Lemmas from Lecture 16.

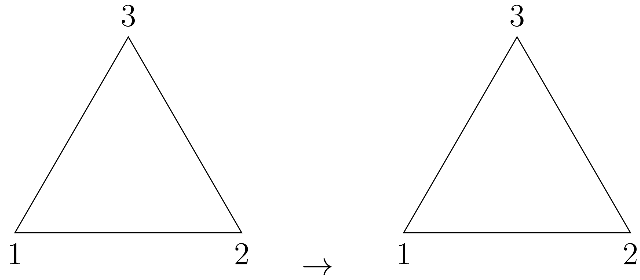
If $\sigma, \tau \in G$ are two different motions of the triangle, define $*(\sigma, \tau)$ to be the motion of the triangle you get by applying σ first, then applying τ. For example if σ is rotation anti-clockwise by $\frac{2\pi}{3}$ radians, and τ is a flip through a vertical centre line, then $*(\sigma, \tau)$ is



(a) Is $*(\sigma, \tau)$ the same motion as $*(\tau, \sigma)$?

(b) What is $*(\tau, \tau)$?

(c) Write down all possible motions of the triangle, including the motion "do nothing" (which you can call "e"). Hint, there should be exactly 6 motions (including e).



(d) Show that for each motion $x \in G$ there is a motion $y \in G$ so that $*(x, y) = e$.

(e) Explain why G with the operation $*$ is a *group*.

(f) If you happened to label the elements of G by

$$e, a, b, c, d, f$$

where e is the "do nothing" move, and σ, τ are renamed, fill out the entries of the following table where you put $*(x, y)$ in the position which has row labeled by x and column labeled by y. We have done the first column already for you (not very helpful, we just did $*(e, e) = e, *(a, e) = a, *(b, e) = b$ etc!) [3]

$*$	e	a	b	c	d	f
e	e					
a	a					
b	b					
c	c					
d	d					
f	f					

END OF HOMEWORK SHEET 9

[3] Hint: notice that when we did $*(\sigma, \tau)$ above, we got a motion which is just the same as flipping the triangle through a line passing through the bottom left corner. So whatever you called these three motions, you should see this in the table.

Brief solutions:

1. Euclidean algorithm $216 = 43.5 + 1$ so $1 = (-43)5 + 216$ so $d = -43 \equiv 173$.

2. (try dividing by $3, 7, 11, 13, 17, 19, \dots$)
$2223 = 3.3.13.19$ so $\phi(2223) = \phi(9)\phi(13)\phi(19) = (9-3)(12)(18) = 6.12.18 = 1296$.

3. Direct proof. If $n \mid ab$ then $\exists s \in \mathbb{Z}$ so that $ab = sn$. Now a, n relatively prime means $\exists p, q \in \mathbb{Z}$ (Euclidean algorithm backwards!) so that
$$1 = pa + qn$$
Multiply through by b:
$$b = pab + qbn$$
The right hand side is $psn + qn = n(ps + q)$ so we have shown that n divides b.

4. Direct proof. $ab \equiv ac \mod n$ means n divides $ab - ac = a(b - c)$. By Question 5 since $\gcd(a, n) = 1$ this means $n \mid (b - c)$ hence the result.