Upload to Canvas before Feb/23, 6:00pm

Use wolfram alpha (or google search) for modular exponentiation.

Exercise 5.1. [6pts] Compute ALL distinct powers of 2 modulo $n = 29$ to find $\log_2(21)$.

Solution:

$$
\begin{array}{cccc}
2^1 \equiv_{29} 2 & 2^2 \equiv_{29} 4 & 2^3 \equiv_{29} 8 & 2^4 \equiv_{29} 16 \\
2^5 \equiv_{29} 3 & 2^6 \equiv_{29} 6 & 2^7 \equiv_{29} 12 & 2^8 \equiv_{29} 24 \\
2^9 \equiv_{29} 19 & 2^{10} \equiv_{29} 9 & 2^{11} \equiv_{29} 18 & 2^{12} \equiv_{29} 7 \\
2^{13} \equiv_{29} 14 & 2^{14} \equiv_{29} 28 & 2^{15} \equiv_{29} 27 & 2^{16} \equiv_{29} 25 \\
2^{17} \equiv_{29} \mathbf{21} & 2^{18} \equiv_{29} 13 & 2^{19} \equiv_{29} 26 & 2^{20} \equiv_{29} 23 \\
2^{21} \equiv_{29} 17 & 2^{22} \equiv_{29} 5 & 2^{23} \equiv_{29} 10 & 2^{24} \equiv_{29} 20 \\
2^{25} \equiv_{29} 11 & 2^{26} \equiv_{27} 22 & 2^{27} \equiv_{28} 15 & 2^{28} \equiv_{29} 1
\end{array}
$$

Hence, $\log_2(21) = 17$. □

Exercise 5.2. [2pts] Use computations done in Exercise 5.1 to solve an instance $n = 29$, $g = 2$, $A = 18$, $B = 14$ of CDH.

Solution: Clearly, $a = \log_2(18) = 11$ and $b = \log_2(14) = 13$. Hence, $2^{11 \cdot 13} = 2^{143} \equiv_{29} 2^3 \equiv_{29} 8$. □

Exercise 5.3. [2pts] Suppose that Bob sends a message to Alice using ElGamal protocol. For public information collected by Eve $n = 29$, $g = 2$, $A = 17$, $c_1 = 6$ and $c_2 = 10$ find m. Use computations done in Exercise 5.1.

Solution: $a = \log_2(17) = 21$ and, hence, $\frac{c_2}{c_1^a} = \frac{10}{6^{21}} \equiv_{29} 10 \cdot 6^7 \equiv_{29} 19$. □

Exercise 5.4. [10pts] For $n = 37$ use the babystep-giantstep algorithm to compute $\log_2(3)$ modulo n. I expect to see the list of babysteps, the list of giantsteps, and a matching pair.

Solution: First, we compute $N = |2|$. Since $\varphi(37) = 36 = 2^2 \cdot 3^2$ we compute $2^{18} \equiv_{37} 36$ and $2^{12} \equiv_{37} 26$, and conclude that $|2| = 36 = N$. Hence, $n = 1 + \lfloor\sqrt{N}\rfloor = 7$. Then compute babysteps

$$
\begin{array}{cccc}
2^0 \equiv_{37} 1 & 2^1 \equiv_{37} 2 & 2^2 \equiv_{37} 4 & 2^3 \equiv_{37} 8 \\
2^4 \equiv_{37} 16 & 2^5 \equiv_{37} \mathbf{32} & 2^6 \equiv_{37} 27 & 2^7 \equiv_{37} 17.
\end{array}
$$

Then compute $g^{-n} = 2^{-7} \equiv 24$ and the list of giantsteps

$$
\begin{array}{ccc}
3 \equiv_{37} 3 & 3 \cdot 2^{-7} \equiv_{37} 3 \cdot 24 \equiv_{37} 35 & 3 \cdot 2^{-7 \cdot 2} \equiv_{37} 3 \cdot 24^2 \equiv_{37} 26 \\
3 \cdot 2^{-7 \cdot 3} \equiv_{37} 3 \cdot 24^3 \equiv_{37} \mathbf{32} & 3 \cdot 2^{-7 \cdot 4} \equiv_{37} 3 \cdot 24^4 \equiv_{37} 28 & 3 \cdot 2^{-7 \cdot 5} \equiv_{37} 3 \cdot 24^5 \equiv_{37} 6 \\
3 \cdot 2^{-7 \cdot 6} \equiv_{37} 3 \cdot 24^6 \equiv_{37} 33 & 3 \cdot 2^{-7 \cdot 7} \equiv_{37} 3 \cdot 24^7 \equiv_{37} 15. &
\end{array}
$$

Find a matching pair $2^5 \equiv_{37} h2^{-7 \cdot 3} = h2^{-21}$ and conclude that $h = 2^{26}$ and $\log_2(3) = 26$.

□

Exercise 5.5. [10pts] Use Pohlig–Hellman algorithm to compute $\log_2(19)$ modulo 37. Compute x_i's directly, by computing sufficiently many powers of g_i.

Solution: We've seen above that $|2| = 36 = 2^2 \cdot 3^2 = N$ and hence

$$N_1 = 9 \quad \text{and} \quad N_2 = 4$$

$$
\begin{array}{ccc}
g_1 = 2^9 \equiv_{37} 31 & \text{and} & g_2 = 2^4 \equiv_{37} 16 \\
h_1 = 19^9 \equiv_{37} 6 & \text{and} & h_2 = 19^4 \equiv_{37} 7
\end{array}
$$

Then we directly compute $x_1 = \log_{g_1}(h_1) = \log_{31}(6) = 3$ as follows:

$$31^2 \equiv_{37} 36 \qquad\qquad 31^3 \equiv_{37} 6$$

and compute $x_2 = \log_{g_2}(h_2) = \log_{16}(7) = 8$ as follows:

$$16^2 \equiv_{37} 34 \qquad 16^3 \equiv_{37} 26 \qquad 16^4 \equiv_{37} 9 \qquad 16^5 \equiv_{37} 33 \qquad 16^6 \equiv_{37} 10 \qquad 16^7 \equiv_{37} 12 \qquad 16^8 \equiv_{37} 7$$

Finally, solve the following system of congruences:

$$\begin{cases} x \equiv_4 3 \\ x \equiv_9 8 \end{cases}$$

to get $x \equiv_{36} 35$.

□

Exercise 5.6. [10pts] For $N = 43$ and $g = 5$ compute $|g|$, choose $B = 3$. Compute B-smooth powers $g^i \,\%\, 43$ for $i = 1, \ldots, 15$ and use them to compute $\log_5(2)$ and $\log_5(3)$.

Solution: $\varphi(43) = 42 = 2 \cdot 3 \cdot 7$. Directly check that $5^{21} \equiv_{43} 42$, $5^{14} \equiv_{43} 36$, $5^6 \equiv_{43} 16$. Hence, $|5| = 42$ in U_{43}.

$$\begin{array}{ccc}
5^1 \equiv_{43} 5 & \Rightarrow & \text{(discard)} \\
5^2 \equiv_{43} 25 & \Rightarrow & \text{(discard)} \\
5^3 \equiv_{43} 39 & \Rightarrow & \text{(discard)} \\
5^4 \equiv_{43} 23 & \Rightarrow & \text{(discard)} \\
5^5 \equiv_{43} 29 & \Rightarrow & \text{(discard)} \\
5^6 \equiv_{43} 2^4 & \Rightarrow & 6 \equiv_{42} 4\log_5(2) \\
5^7 \equiv_{43} 37 & \Rightarrow & \text{(discard)} \\
5^8 \equiv_{43} 13 & \Rightarrow & \text{(discard)} \\
5^9 \equiv_{43} 22 & \Rightarrow & \text{(discard)} \\
5^{10} \equiv_{43} 2^3 \cdot 3 & \Rightarrow & 10 \equiv_{42} 3\log_5(2) + \log_5(3) \\
5^{11} \equiv_{43} 34 & \Rightarrow & \text{(discard)} \\
5^{12} \equiv_{43} 41 & \Rightarrow & \text{(discard)} \\
5^{13} \equiv_{43} 33 & \Rightarrow & \text{(discard)} \\
5^{14} \equiv_{43} 2^2 \cdot 3^2 & \Rightarrow & 14 \equiv_{42} 2\log_5(2) + 2\log_5(3) \\
5^{15} \equiv_{43} 2^3 & \Rightarrow & 15 \equiv_{42} 3\log_5(2).
\end{array}$$

Subtracting $15 \equiv_{42} 3\log_5(2)$ from $6 \equiv_{42} 4\log_5(2)$ we get

$$6 - 15 \equiv_{42} \log_5(2)$$

and $\log_5(2) \equiv_{42} -9 \equiv_{42} 33$. Similarly, subtracting $10 \equiv_{42} 3\log_5(2) + \log_5(3)$ from $14 \equiv_{42} 2\log_5(2) + 2\log_5(3)$ we get

$$4 \equiv_{42} -\log_5(2) + \log_5(3)$$

and $\log_5(3) \equiv_{42} -5 \equiv_{42} 37$.

□

A **ring** is a set R with two binary operations $+$ and $\cdot$, called **addition** and **multiplication**, that satisfy the following axioms:

(R1) (R,+) is an abelian group with identity denoted by 0.
(R2) Multiplication is associative and R contains 1 (**unity**).
(R3) $(a+b)c = ac+bc$ and $c(a+b) = ca+cb$.

To check if $(R,+,\cdot)$ is a ring it is sufficient to check that $+$ and $\cdot$ are indeed binary functions on R and that all axioms (R1), (R2), (R3) are satisfied.

Exercise 5.7. [+12pts] Which of the following are rings? EXPLAIN!

(1) $(\mathbb{Z},+,\cdot)$
(2) $(\mathbb{Z}_n,+,\cdot)$.
(3) $(U_n,+,\cdot)$.
(4) $(\mathbb{N},+,\cdot)$.
(5) $\{a+b\sqrt{5} \mid a,b\in\mathbb{Z}\}$ with standard addition and multiplication.
(6) The set of all real-valued functions $\mathbb{R}^{\mathbb{R}} = \{f:\mathbb{R}\to\mathbb{R}\}$ with $+,\cdot$ defined as follows:

$$(f+g)(x) = f(x)+g(x),$$
$$(f\cdot g)(x) = f(x)\cdot g(x).$$

Solution: Straightforward check of axioms.

---

(1) $(\mathbb{Z},+,\cdot)$ is a ring, because $+,\cdot$ are binary functions on $\mathbb{Z}$ and (R1), (R2), (R3) hold.
  (R1) $(\mathbb{Z},+)$ is an abelian group
    (G1) 0 is the additive identity.
    (G2) $-n$ is the inverse of n.
    (G3) $+$ is associative.
    – $+$ is commutative.
  (R2) Multiplication is associative and $\mathbb{Z}$ contains 1.
  (R3) $(a+b)c = ac+bc$ and $c(a+b) = ca+cb$ hold in $\mathbb{Z}$.

---

(2) $(\mathbb{Z}_n,+,\cdot)$ is a ring, because $+,\cdot$ are binary functions on $\mathbb{Z}_n$ and (R1), (R2), (R3) hold.
  (R1) $(\mathbb{Z}_n,+)$ is an abelian group:
    (G1) $[0]$ is the additive identity.
    (G2) $[-n]$ is the inverse of $[n]$.
    (G3) $+$ is associative.
    – $+$ is commutative.
  (R2) Multiplication is associative and $\mathbb{Z}_n$ contains $[1]$.
  (R3) $(a+b)c = ac+bc$ and $c(a+b) = ca+cb$ hold in $\mathbb{Z}_n$.

---

(3) $(U_n,+,\cdot)$ is not a ring. With every $[a]$ it contains $[-a]$, but does not contain $[a]+[-a]=[0]$. Hence, $+$ is not a binary operation on U_n. In other words, U_n is nor closed nuder $+$.

---

(4) $(\mathbb{N},+,\cdot)$ is not a ring (even if we assume that $0\in\mathbb{N}$) because $(\mathbb{N},+)$ is not an abelian group, with $\mathbb{N}$ has no additive inverses.

---

(5) $R=\{a+b\sqrt{5} \mid a,b\in\mathbb{Z}\}$ is a ring. R is closed under $+$ and $\cdot$ because for any $a,b,c,d\in\mathbb{Z}$ we have

$$(a+b\sqrt{5})+(c+d\sqrt{5}) = (\underbrace{a+c}_{\in\mathbb{Z}})+(\underbrace{b+d}_{\in\mathbb{Z}})\sqrt{5}\in R$$
$$(a+b\sqrt{5})\cdot(c+d\sqrt{5}) = (\underbrace{ac+5bd}_{\in\mathbb{Z}})+(\underbrace{bc+ad}_{\in\mathbb{Z}})\sqrt{5}\in R$$

Check that (R1), (R2), (R3) hold:
  (R1) $(R,+)$ is an abelian group:
    (G1) $0 = 0+0\sqrt{5}\in R$.
    (G2) $-(a+b\sqrt{5}) = -a-b\sqrt{5}$.
    (G3) $+$ is associative.

- $+$ is commutative.

(R2) Multiplication is associative and R contains $1 = 1 + 0\sqrt{5}$.

(R3) $(a+b)c = ac + bc$ and $c(a+b) = ca + cb$ hold in R.

---

(6) The set of all real-valued functions $\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}$ is a ring. It is obvious that the sum and the product of real-valued functions are real-valued functions and, hence, $\mathbb{R}^{\mathbb{R}}$ is closed under $+, \cdot$. Check that (R1), (R2), (R3) hold:

(R1) $(\mathbb{R}^{\mathbb{R}}, +)$ is an abelian group:

(G1) the constant function 0 is the additive identity.

(G2) $-f(x)$ is the additive inverse for $f(x)$.

(G3) $+$ is associative.

- $+$ is commutative.

(R2) Multiplication is associative and R contains the constant function 1.

(R3) $(a+b)c = ac + bc$ and $c(a+b) = ca + cb$ hold in $\mathbb{R}^{\mathbb{R}}$.

$\square$