---

1. Two of the following six integers are prime and the other four are composite:

$$\begin{aligned}
N_1 &= 14745122888736358662532345696652590572098984231276050977595866277545953667762 4741\\
N_2 &= 18172448673260737423503440134443993127014514156537287438135064627663276632896 9281\\
N_3 &= 25842412674017835212810037073688990681760751808680663275203875878855570430460 4649\\
N_4 &= 32423465792834705112311323202340971023401238975123984712039847191766565558120 0339\\
N_5 &= 40886997116432824752426545058382393043440684430314281684135187943954481868570 2841\\
N_6 &= 54240818463494325767269883491740461154224822887333745936821062491040693758294 2097
\end{aligned}$$

(a) Try the Fermat test with $a = 2, 3, 5$ for each of these integers. (Stop if you find the integer is composite.)

- We compute 2^n, 3^n, and 5^n modulo n for each integer using successive squaring / PowerMod.
- Mod N_1, we get

$$2^n \equiv 88316535944373664491052782881734905472870246733301741951254518347811266513946105.$$

The test shows $\boxed{N_1 \text{ is composite}}$.

- Mod N_2, we get $2^n \equiv 2$, $3^n \equiv 3$, and

$$5^n \equiv 18172448673260737423503440134443993126995449818797276253878997501420650171551774 6.$$

The test shows $\boxed{N_2 \text{ is composite}}$.

- Mod N_3, N_4, N_5, N_6 we get $2^n \equiv 2$, $3^n \equiv 3$, and $5^n \equiv 5$. The $\boxed{\text{test fails}}$ for each.

(b) Try the Miller-Rabin test with $a = 2, 3, 5$ for each of the integers not already identified as composite in part (a). (Stop if you find the integer is composite.)

- For $n = N_3$ we have $n - 1 = 2^3 d$ where d is odd, so with $j = (n-1)/2^3$ we need to compute a^j, a^{2j}, a^{4j}, a^{8j} mod N_3. With $a = 2$ we obtain

$$\begin{aligned}
a^j &\equiv 56509958676279000393051591057362333462754988367560892625850422242578858985275090\\
a^{2j} &\equiv 25842412674017835212810037073688990681760751808680663275203875878855570430460 4648\\
a^{4j} &\equiv 1\\
a^{8j} &\equiv 1
\end{aligned}$$

so since we have an entry of 1 preceded by an entry not ± 1, $\boxed{N_3 \text{ is composite}}$.

- For $n = N_4$ we have $n - 1 = 2d$ where d is odd, so with $j = (n-1)/2$ we need to compute a^j, a^{2j} mod N_3. With $a = 2$ and $a = 3$ we get $a^j \equiv -1$, $a^{2j} \equiv 1$ while with $a = 5$ we get $a^j \equiv 1$, $a^{2j} \equiv 1$, so the $\boxed{\text{test fails}}$.
- For $n = N_5$ we have $n - 1 = 2^3 d$ where d is odd, so with $j = (n-1)/2^3$ we need to compute a^j, a^{2j}, a^{4j}, a^{8j} mod N_3. With $a = 2$ we obtain

$$\begin{aligned}
a^j &\equiv 72562037354213358769539459660115843591087236202395767229215492118756808134486142\\
a^{2j} &\equiv 40040597713960661553371029426656890045444683368161716 89\\
a^{4j} &\equiv 1\\
a^{8j} &\equiv 1
\end{aligned}$$

so since we have an entry of 1 preceded by an entry not ± 1, $\boxed{N_5 \text{ is composite}}$.

- For $n = N_6$ we have $n - 1 = 2^4 d$ where d is odd, so with $j = (n-1)/2$ we need to compute a^j, a^{2j}, a^{4j}, a^{8j}, a^{16j} mod N_3.

With $a = 2$ we obtain

$$\begin{aligned} a^j &\equiv 4960756402679058627690363921033767150779475286241902096016833396668842370394099 47 \\ a^{2j} &\equiv 2534565237620067956931510579653135715176837921559470430208687959903465362193030 47 \\ a^{4j} &\equiv -1 \\ a^{8j} &\equiv 1 \\ a^{16j} &\equiv 1 \end{aligned}$$

With $a = 3$ we obtain

$$\begin{aligned} a^j &\equiv 4596399502983138677135003056792351759730840281669809255469942260154416489232573 74 \\ a^{2j} &\equiv 3399682689124613880063576451474563945857845494509913377591158157843280400899148 46 \\ a^{4j} &\equiv 2889516608729364619795477769520910400245644367173904163473418289200604013636390 50 \\ a^{8j} &\equiv -1 \\ a^{16j} &\equiv 1 \end{aligned}$$

With $a = 5$ we obtain

$$\begin{aligned} a^j &\equiv 8276823433662938995919852923816943556916420070635653382121639889496528865968472 3 \\ a^{2j} &\equiv 3399682689124613880063576451474563945857845494509913377591158157843280400899148 46 \\ a^{4j} &\equiv 2889516608729364619795477769520910400245644367173904163473418289200604013636390 50 \\ a^{8j} &\equiv -1 \\ a^{16j} &\equiv 1 \end{aligned}$$

so the $\boxed{\text{test fails}}$.

(c) Your results from parts (a)-(b) should have identified the four composite numbers. Why don't the results prove that the remaining two integers are actually prime?

- A single application of the Fermat test or the Miller-Rabin test only has the outcomes "n is composite" or "the test is inconclusive": the tests do not say anything in the inconclusive case.

---

2. Factor the given integers using the stated procedure, making sure to give enough detail to show that you did actually use that method (just giving the factorization is not sufficient!):

(a) $N = 1084055561$ by looking for a Fermat factorization.

- We can compute numerically that $\sqrt{N} \approx 32924.999$.
- We then compute $32925^2 - N = 64 = 8^2$.
- Hence we get the factorization $N = (32925 - 8)(32925 + 8) = \boxed{32917 \cdot 32933}$.

(b) $N = 5686741440097$ by looking for a Fermat factorization.

- We can compute numerically that $\sqrt{N} \approx 2384688.96$.
- We then compute $2384689^2 - N = 186624$, which is 432^2.
- Hence we get the factorization $N = (2384689 - 432) \cdot (2384689 + 432) = \boxed{2384257 \cdot 2385121}$.

(c) $N = 1032899106233$ by using Pollard's $(p-1)$-algorithm with $a = 2$.

- Here is a table of the values $x_j = a^{j!} \bmod N$ obtained from applying the algorithm:

j	1	2	3	4	5	6	7	8
$x_j \bmod N$	2	4	64	16777216	827753680774	127266001140	132531396310	333255027817
$\gcd(x_j - 1, N)$	1	1	1	1	1	1	1	604801

- At the 8th step we obtain the divisor 604801 which gives the factorization $N = \boxed{604801 \cdot 1707833}$.

(d) $N = 12038459$ by using Pollard's $(p-1)$-algorithm with $a = 2$.

- Here is a table of the values $x_j = a^{j!} \bmod N$ obtained from applying the algorithm:

j	1	2	3	4	5	6	7	8	9	10	11	12
$x_j \bmod N$	2	4	64	4738757	3931373	9318345	815841	8692063	7723968	4433592	11887022	5685234
$\gcd(x_j - 1, N)$	1	1	1	1	1	1	1	1	1	1	1	2917

- At the 12th step we obtain the divisor 2917 which gives the factorization $N = \boxed{2917 \cdot 4127}$.

(e) $N = 1626641013131$ by using Pollard's ρ-algorithm with $a = 2$ and $p(x) = x^2 + 1$.

- We start with $u = 2$, so that $x_1 = y_1 = 2$, and successively keep track of the terms $x_i = p(x_{i-1})$ and $y_i = p(p(y_i))$ modulo N.

i	1	2	3	4	5	6	7	8
$x_i \bmod N$	2	5	26	677	458330	210066388901	1075666426770	1005009459326
$y_i \bmod N$	2	26	458330	1075666426770	1247681323453	1487579551298	340467499342	1217658160841
$\gcd(y_i - x_i, N)$	N	1	1	1	1	1	1	122011

- At the 8th step we obtain a nontrivial divisor 122011, yielding $N = \boxed{122011 \cdot 13331921}$.

(f) $N = 12038459$ by using Pollard's ρ-algorithm with $a = 2$ and $p(x) = x^2 + 1$.

- We start with $u = 2$, so that $x_1 = y_1 = 2$, and successively keep track of the terms $x_i = p(x_{i-1})$ and $y_i = p(p(y_i))$ modulo N.

i	1	2	3	4	5	6	7	8	9	10	11	12
$x_i \bmod N$	2	5	26	677	458330	7317810	3103253	1866501	4294533	10230877	6567994	3434191
$y_i \bmod N$	2	26	458330	3103253	4294533	6567994	10888247	8076085	429847	54748	4217838	1696724
$\gcd(y_i - x_i, N)$	N	1	1	1	1	1	1	1	1	1	1	4127

- At the 12th step we obtain a nontrivial divisor 4127, yielding $N = \boxed{4127 \cdot 2917}$.

---

3. Generate (however you like) three 10-digit, three 20-digit, three 30-digit, and three 40-digit numbers: one number should be prime, another should be a product of two primes of roughly equal sizes, and the third should be a product of three primes of roughly equal sizes.

(a) List the numbers you generated and briefly mention how you generated them.

- Approaches may vary, but Mathematica code was provided to do this automatically.

(b) Use the Fermat test (with three residues $a = 2, 3, 5$) and the Miller-Rabin test (with three residues $a = 2, 3, 5$) to test the primality of your integers. How effective are the tests?

- This depends on the integers chosen, but usually the Fermat test will suffice to show the composite values are composite.

(c) Do the primality testing algorithms take noticeably longer for the larger numbers than the small ones? Briefly explain.

- No: they only involve successive squaring, which is very efficient even for large values. The larger ones do take a bit longer, but the times should all be fractions of a millisecond.

(d) Factor the composite numbers using the Pollard $(p-1)$- and ρ-algorithms, stopping after a maximum of 1,000,000 steps. List the number of steps each algorithm takes to find a factor.

- The products of two primes should take roughly 300 steps for 10-digit and 100000 steps for 20-digit two-prime products, and fail for 30-digit and 40-digit products. The products of three primes should take roughly 50, 2000, 10000, and 500000 steps respectively.

(e) Do the algorithms take more steps for the larger numbers than the smaller ones? Briefly explain.

- Yes: substantially more, and in fact the larger calculations usually fail without finding a factor.

(f) Is there a difference between the number of steps for products of two versus three primes? Briefly explain.

- Yes: for N-digit products of two primes Pollard ρ takes roughly $10^{N/4}$ steps, while for N-digit products of three primes it takes roughly $10^{N/6}$ steps.

---

4. Consider the Rabin cryptosystem with key $N = 1359692821 = 32359 \cdot 42019$.

   (a) Encode the plaintext $m = 117285016$.

   - We simply compute $m^2 \pmod N$, which PowerMod gives as $\boxed{654306931}$.

   (b) Find the four decodings of the ciphertext $c = 823845737$.

   - We wish to solve $m^2 \equiv c \pmod p$ and $m^2 \equiv c \pmod q$ and combine the results.
   - Since $p \equiv q \equiv 3 \pmod 4$, we know that the solutions are $m = \pm c^{(p+1)/4} \pmod p$ and $m = \pm c^{(q+1)/4} \pmod q$.
   - We then compute $c^{(p+1)/4} \equiv 32225 \pmod p$ and $c^{(q+1)/4} \equiv 9955 \pmod q$ via PowerMod.
   - Solving the simultaneous congruences $m \equiv 32225 \pmod{32359}$, $m \equiv 9955 \pmod{42019}$ via ChineseRemainder yields $m \equiv 547643582 \pmod N$.
   - Solving $m \equiv 32225 \pmod{32359}$, $m \equiv -9955 \pmod{42019}$ likewise yields $m \equiv 929156192 \pmod N$.
   - Thus the four solutions are ± 547643582 and $\pm 929156192 \pmod N$.
   - Equivalently: $m = \boxed{430536629,\ 547643582,\ 812049239,\ 929156192}$.

---

5. Consider the RSA cryptosystem with key $N = 1085444233 = 31907 \cdot 34019$ and encryption exponent $e = 3$.

   (a) Encrypt the plaintext $m = 277891194$.

   - We simply compute $m^e \pmod N$ using PowerMod: we obtain $\boxed{604479369}$.

   (b) Find a decryption exponent d.

   - We need to solve $de \equiv 1 \pmod{\varphi(N)}$.
   - First we observe $\varphi(N) = 1085378308$.
   - So we want to find the inverse of 3 modulo $\varphi(N)$: this is $\boxed{723585539}$ again via PowerMod.

   (c) Decrypt the ciphertext $c = 878460400$.

   - We simply compute $m^d \pmod N$ using PowerMod, giving $\boxed{605435934}$.

---

6. As proven on homework 2, the only possible primes of the form $a^n - 1$ are the Mersenne numbers $2^p - 1$ where p is a prime. The goal of this problem is to study the prime factorizations of Mersenne numbers.

   (a) Apply the Miller-Rabin test with $a = 2, 3, 5$ on $2^p - 1$ for $p = 11$, 13, 17, 19, 23, 29. You should find that three values are composite: why can you not conclude that the other three values are necessarily prime?

   - For $n = 2^p - 1$ we have $n - 1 = 2(2^{p-1} - 1)$ so with $j = (n-1)/2$ we compute a^j, $a^{2j} \bmod n$.
   - First, $n = 2^{11} - 1$. With $a = 2$ we get {1,1} so the $\boxed{\text{test fails}}$. With $a = 3$ get {1565, 1013} so $\boxed{2^{11} - 1 \text{ is composite}}$.
   - Next, $n = 2^{13} - 1$. With $a = 2$ we get {1,1} so the $\boxed{\text{test fails}}$. With $a = 3$ we get $\{-1, 1\}$ so the $\boxed{\text{test fails}}$. With $a = 5$ we get $\{1, 1\}$ so the $\boxed{\text{test fails}}$.
   - Next, $n = 2^{17} - 1$. With $a = 2$ we get $\{1, 1\}$ so the $\boxed{\text{test fails}}$. With $a = 3$ we get $\{-1, 1\}$ so the $\boxed{\text{test fails}}$. With $a = 5$ we get $\{1, 1\}$ so the $\boxed{\text{test fails}}$.
   - Next, $n = 2^{19} - 1$. With $a = 2$ we get $\{1, 1\}$ so the $\boxed{\text{test fails}}$. With $a = 3$ we get $\{-1, 1\}$ so the $\boxed{\text{test fails}}$. With $a = 5$ we get $\{-1, 1\}$ so the $\boxed{\text{test fails}}$.
   - Next, $n = 2^{23} - 1$. With $a = 2$ we get $\{1, 1\}$ so the $\boxed{\text{test fails}}$. With $a = 3$ we get {7511964, 5884965} so $\boxed{2^{23} - 1 \text{ is composite}}$.
   - Finally, $n = 2^{23} - 1$. With $a = 2$ we get $\{1, 1\}$ so the $\boxed{\text{test fails}}$. With $a = 3$ we get {89777599, 65165529} so $\boxed{2^{29} - 1 \text{ is composite}}$.
   - The point is that a single application of the Miller-Rabin test only has the outcomes "n is composite" or "the test is inconclusive": the tests simply do not say anything in the inconclusive case.

(b) Use Pollard's ρ-algorithm with $a = 3$ and polynomial $p(x) = x^2 + 1$ to find the factorizations of the three values $2^p - 1$ you identitied as composite in part (a). (Note that the largest one has three prime factors; make sure to find all three by extending the computation past where the first prime factor is found.) How many steps are required to find the factorizations?

- Here are the values for $N = 2^{11} - 1$:

Value	$i = 1$	$i = 2$	$i = 3$
$x_i \bmod N$	3	10	101
$y_i \bmod N$	3	101	1090
$\gcd(y_i - x_i, N)$	N	1	23

At the 3rd step we obtain the nontrivial divisor 23, yielding the factorization $2^{11} - 1 = \boxed{23 \cdot 89}$.

- Here are the values for $N = 2^{23} - 1$:

Value	$i = 1$	$i = 2$	$i = 3$	$i = 4$
$x_i \bmod N$	3	10	101	10202
$y_i \bmod N$	3	101	3417521	4093466
$\gcd(y_i - x_i, N)$	N	1	1	47

At the 4th step we obtain the nontrivial divisor 47, yielding the factorization $2^{23} - 1 = \boxed{47 \cdot 178481}$.

- Here are the values for $N = 2^{23} - 1$:

i	1	2	3	4	5	6	7	8	9	10
$x_i \bmod N$	3	10	101	10202	104080805	231014258	526457618	21370981	60560107	305537150
$y_i \bmod N$	3	101	104080805	526457618	60560107	463797792	363923159	24815603	107704659	529315099
$\gcd(y_i - x_i, N)$	N	1	1	1	1	1	1	1	2089	1

At the 9th step we obtain the nontrivial divisor 2089 and at the 11th step we obtain 233, yielding the factorization $2^{29} - 1 = \boxed{233 \cdot 1103 \cdot 2089}$.

---

7. For all of the factorizations in problem 6, notice that all of the prime factors of $2^p - 1$ are congruent to 1 modulo p. The goal is now to prove this fact, which was first established by Euler. Let p be a prime.

(a) Suppose that q is a prime that divides $2^p - 1$. Show that the order of 2 modulo q must equal p.

- If q divides $2^p - 1$ then $2^p \equiv 1 \pmod{q}$. But by properties of order, this means the order of 2 modulo q must divide p, so it is either 1 or p.
- But clearly the order cannot be 1 since $2^1 \not\equiv 1 \pmod{q}$, so the only possibility is that the order equals p.

(b) Suppose that q is a prime that divides $2^p - 1$. Show that $q \equiv 1 \pmod{p}$.

- By (a), the order of 2 modulo q is p. By Euler's theorem, the order of any element modulo q divides $q - 1$.
- Therefore, p divides $q - 1$, which is to say, $q \equiv 1 \pmod{p}$.

---

8. Recall that the Lucas primality criterion says that if $a^{m-1} \equiv 1 \pmod{m}$ and $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for any prime p dividing $m - 1$, then m is prime.

(a) Use the Lucas primality criterion to show that 1013 is prime, and then establish that 2027 is prime. [Hint: Try $a = 7$ for both.]

- First, we have $1013 - 1 = 1012 = 2^2 \cdot 11 \cdot 23$. Now we compute $7^{1012} \equiv 1 \pmod{1013}$, but $7^{1012/2} \equiv -1 \pmod{1013}$, $7^{1012/11} \equiv 840 \pmod{1013}$, and $7^{1012/23} \equiv 990 \pmod{1013}$. So by part (b), this means 1013 is prime.
- For 2027, we have $2026 = 2 \cdot 1013$ and 1013 is prime by the above. Now we compute $7^{2026} \equiv 1 \pmod{2027}$ but $7^{2026/2} \equiv -1 \pmod{2027}$ and $7^2 \equiv 49 \pmod{2027}$. So by part (b), this means 2027 is prime.

(b) Use the Lucas primality criterion with $a = 10$ to show that the integer

$$N = 84315678462027496382807904466449937832017712702684073443683333522259304931292723538748961587 3$$

is prime. (If writing by hand, you can just give the first three and last three digits of any large values.)

- To apply the criterion we first need to factor $N - 1$.
- Using FactorInteger produces the factorization $N-1 = 2^{15}3^{13}7^{12}11^{13}13 \cdot 1013^7 2027^{11}$, and 1013 and 2027 are prime by (a).
- Then we must compute the following values modulo N:

$$\begin{aligned}
a^{N-1} &\equiv 1 \\
a^{(N-1)/2} &\equiv -1 \\
a^{(N-1)/3} &\equiv 709729274263082829289661469978323780615812896318322643728828803685814166253235090218971573 28 \\
a^{(N-1)/7} &\equiv 511988274222857596429898210663052019771207667414886091839314224693774536755678906794441864857 \\
a^{(N-1)/11} &\equiv 736908042641603289170515640322561601868923881259488267995239604664349446884174116046604565017 \\
a^{(N-1)/13} &\equiv 459504551413244721489438239305022768327589729306817216271694350492982930307794167935207965709 \\
a^{(N-1)/1013} &\equiv 736157845610144004762183977115470779366440984764453242434674106757868687336658309503192600 70 \\
a^{(N-1)/2027} &\equiv 901572120899637776275344460956505179240965069310204835660786847304328732640222061606010326 28
\end{aligned}$$

- Since $a^{N-1} \equiv 1$ but $a^{(N-1)/q} \not\equiv 1$ for any prime divisor q of $N-1$, the Lucas criterion therefore says that N is prime.
