---

1. 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 $N = \boxed{4127 \cdot 2917}$.

---

2. 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) 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.

   (b) 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.

   (c) 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.

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

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

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

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

---

3. For each element in each ring $\mathbb{Z}[\sqrt{D}]$, (i) determine whether it is a unit and if so find its multiplicative inverse, and (ii) if it is not a unit, determine whether it is irreducible or reducible, and (iii) if it is reducible, find a nontrivial factorization.

   (a) The elements $-i$, $3+2i$, $1+i$, and $1+5i$ in $\mathbb{Z}[i]$.

   - The norm of an element here is $N(a+bi) = a^2+b^2$. Additionally recall that an element is a unit if and only if its norm is ± 1, while if its norm is $\pm p$ where p is prime then it is irreducible.
   - Since $N(-i) = 0^2 + (-1)^2 = 1$, we see $-i$ $\boxed{\text{is a unit}}$. The norm map calculation says $i(-i) = 1$, so the multiplicative inverse is $\boxed{i}$.
   - Since $N(3+2i) = 3^2+2^2 = 13$, we see $3+2i$ is $\boxed{\text{irreducible}}$.
   - Since $N(1+i) = 1^2+1^2 = 2$, we see $1+i$ is $\boxed{\text{irreducible}}$.
   - Since $N(1+5i) = 1^2+5^2 = 26$ is not prime, we see $1+5i$ may be reducible. If it is reducible, it would factor into a product of elements of smaller norm, and searching for elements of norms 2 and 13 will eventually yield a nontrivial factorization $\boxed{1+5i = (3+2i)(1+i)}$ (note that these are just the two previous irreducible elements we listed!).

   (b) The elements $1+2\sqrt{5}$, $9+4\sqrt{5}$, $5+\sqrt{5}$, $21+4\sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$.

   - The norm of an element here is $N(a+b\sqrt{5}) = a^2-5b^2$. Additionally, an element is a unit if and only if its norm is ± 1, while if its norm is $\pm p$ where p is prime then it is irreducible.
   - Since $N(1+2\sqrt{5}) = 1^2-5\cdot 2^2 = -19$, we see $1+2\sqrt{5}$ is $\boxed{\text{irreducible}}$.
   - Since $N(9+4\sqrt{5}) = 9^2-5\cdot 4^2 = 1$, we see $9+4\sqrt{5}$ $\boxed{\text{is a unit}}$. The norm map calculation says $(9+4\sqrt{5})(9-4\sqrt{5}) = 1$, so the multiplicative inverse is $\boxed{9-4\sqrt{5}}$.
   - Since $N(5+\sqrt{5}) = 5^2-5\cdot 1^2 = 20$ is not prime, we see $5+\sqrt{5}$ may be reducible. If it is reducible, it would factor into a product of elements of smaller norm, and searching for elements of norms ± 2, ± 4, ± 5, and ± 5 will eventually yield a nontrivial factorization $\boxed{5+\sqrt{5} = \sqrt{5}(1+\sqrt{5})}$, where $N(\sqrt{5}) = -5$ and $N(1+\sqrt{5}) = -4$.

- Since $N(21+4\sqrt{5}) = 21^2 - 5 \cdot 4^2 = 361 = 19^2$ is not prime, we see $21+4\sqrt{5}$ may be reducible. If it is reducible, it would factor into a product of elements of smaller norm, so searching for elements of norm ± 19 eventually yields the factorization $\boxed{21+4\sqrt{5} = (1+2\sqrt{5})^2}$, using the element $1+2\sqrt{5}$ from earlier.

---

4. Use the Euclidean algorithm in each Euclidean domain to compute a greatest common divisor of each pair of elements, and then to write it as a linear combination of the elements:

   (a) The polynomials $x^6 - 1$ and $x^8 - 1$ in $\mathbb{R}[x]$.

   - We apply the Euclidean algorithm.
   - Dividing $x^6 - 1$ into $x^8 - 1$ yields $x^8 - 1 = x^2(x^6 - 1) + (x^2 - 1)$: the quotient is x^2 and the remainder is $x^2 - 1$.
   - Dividing $x^2 - 1$ into $x^6 - 1$ yields $x^6 - 1 = (x^4 + x^2 + 1)(x^2 - 1) + 0$: the quotient is $x^4 + x^2 + 1$ and the remainder is 0.
   - The last nonzero remainder is $\boxed{x^2 - 1}$, so it is the gcd.
   - Solving the first equation gives $\boxed{x^2 - 1 = 1(x^8 - 1) - x^2(x^6 - 1)}$.

   (b) The elements $11 + 27i$ and $-9 + 7i$ in $\mathbb{Z}[i]$.

   - We apply the Euclidean algorithm.
   - First, $\dfrac{11+27i}{-9+7i} = \dfrac{9}{13} - \dfrac{32}{13}i$ so rounding to the nearest Gaussian integer yields the quotient $q = 1 - 2i$ with remainder $r = (11 + 27i) - (1 - 2i)(-9 + 7i) = 6 + 2i$.
   - Next, $\dfrac{-9+7i}{6+2i} = -1 + \dfrac{3}{2}i$ so rounding yields the quotient $q = -1 + 2i$ with remainder $r = (-9 + 7i) - (-1 + 2i)(6 + 2i) = 1 - 3i$.
   - Finally, we have $\dfrac{6+2i}{1-3i} = 2i$ with quotient $2i$ and remainder 0. The last nonzero remainder $\boxed{1 - 3i}$ is a gcd.
   - To express the gcd as a linear combination, we solve for the remainders:

$$\begin{aligned} 6 + 2i &= 1 \cdot (11 + 27i) + (-1 + 2i) \cdot (-9 + 7i) \\ 1 - 3i &= (-9 + 7i) + (1 - 2i) \cdot (6 + 2i) \\ &= (1 - 2i) \cdot (11 + 27i) + (4 + 4i) \cdot (-9 + 7i) \end{aligned}$$

     and thus we obtain $1 - 3i = \boxed{(1 - 2i) \cdot (11 + 27i) + (4 + 4i) \cdot (-9 + 7i)}$.
   - Note here that there are four possible gcds: $1 - 3i$ and its associates $3 + i$, $-1 + 3i$, and $-3 - i$.

   (c) The polynomials $x^3 + x^2 + 1$ and $x^4 + x$ in $\mathbb{R}[x]$.

   - We apply the Euclidean algorithm.
   - Dividing $x^3 + x^2 + 1$ into $x^4 + x$ yields $x^4 + x = (x - 1)(x^3 + x^2 + 1) + (x^2 + 1)$: the quotient is $x - 1$ and the remainder is $x^2 + 1$.
   - Dividing $x^2 + 1$ into $x^3 + x^2 + 1$ yields $x^3 + x^2 + 1 = (x + 1)(x^2 + 1) + (-x)$: the quotient is $x + 1$ and the remainder is $-x$.
   - Dividing $-x$ into $x^2 + 1$ yields $x^2 + 1 = (-x)(-x) + 1$: the quotient is $-x$ and the remainder is 1.
   - Finally, $-x = (-x)(1)$. The last nonzero remainder is $\boxed{1}$, so it is a gcd. To express the gcd as a linear combination, we solve for the remainders:

$$\begin{aligned} x^2 + 1 &= (x^4 + x) + (1 - x)(x^3 + x^2 + 1) \\ -x &= (x^3 + x^2 + 1) - (x + 1)(x^2 + 1) \\ &= (-x - 1)(x^4 + x) + (x^2)(x^3 + x^2 + 1) \\ 1 &= (x^2 + 1) - (-x)(-x) \\ &= (-x^2 - x + 1)(x^4 + x) + (x^3 - x + 1)(x^3 + x^2 + 1) \end{aligned}$$

- Thus we have $1 = \boxed{(-x^2 - x + 1)(x^4 + x) + (x^3 - x + 1)(x^3 + x^2 + 1)}$.

(d) The elements $43 - i$ and $50 - 50i$ in $\mathbb{Z}[i]$.

- We use the Euclidean algorithm:

$$\begin{aligned} 50 - 50i &= (1 - i) \cdot (43 - i) + (8 - 6i) \\ 43 - i &= (4 + 2i) \cdot (8 - 6i) + (-1 + 7i) \\ 8 - 6i &= (-1 - i) \cdot (-1 + 7i) \end{aligned}$$

- The last nonzero remainder is $\boxed{-1 + 7i}$ so it is a gcd. To express the gcd as a linear combination, we solve for the remainders:

$$\begin{aligned} 8 - 6i &= 1 \cdot (50 - 50i) + (-1 + i) \cdot (43 - i) \\ -1 + 7i &= 43 - i + (-4 - 2i) \cdot (8 - 6i) \\ &= (-4 - 2i)(50 - 50i) + (7 - 2i)(43 - i) \end{aligned}$$

- Thus we have $-1 + 7i = \boxed{(-4 - 2i)(50 - 50i) + (7 - 2i)(43 - i)}$.
- Note here that there are four possible gcds: $-1 + 7i$ and its associates $-7 - i$, $1 - 7i$, and $7 + i$.

(e) The elements $x^4 + 2x + 1$ and $x^3 + x$ in $\mathbb{F}_3[x]$.

- We apply the Euclidean algorithm: we have

$$\begin{aligned} x^4 + 2x + 1 &= x(x^3 + x) + (2x^2 + 2x + 1) \\ x^3 + x &= (2x + 1)(2x^2 + 2x + 1) + 2 \\ 2x^2 + 2x + 1 &= (x^2 + x + 2)(2) \end{aligned}$$

  and so the last nonzero remainder is 2. Thus, by rescaling, we see that the gcd is $\boxed{1}$.
- By back-solving, we see that

$$\begin{aligned} 2x^2 + 2x + 1 &= 1 \cdot (x^4 + 2x + 1) - x \cdot (x^3 + x) \\ 2 &= (x^3 + x) - (2x + 1)(2x^2 + 2x + 1) \\ &= (2x^2 + x + 1) \cdot (x^3 + x) - (2x + 1)(x^4 + 2x + 1) \end{aligned}$$

  and thus by rescaling, we obtain $1 = \boxed{(x^2 + 2x + 2) \cdot (x^3 + x) - (x + 2)(x^4 + 2x + 1)}$.

(f) The elements $9 + 43i$ and $22 + 10i$ in $\mathbb{Z}[i]$.

- First, $\dfrac{9 + 43i}{22 + 10i} = \dfrac{157}{146} + \dfrac{107}{73}i$, so rounding to the nearest Gaussian integer yields the quotient $1 + i$, and the remainder is then $(9 + 43i) - (1 + i)(22 + 10i) = -3 + 11i$.
- Next, $\dfrac{22 + 10i}{-3 + 11i} = \dfrac{22}{65} - \dfrac{136}{65}i$, so rounding to the nearest Gaussian integer yields the quotient $-2i$, and the remainder is then $(22 + 10i) - (-2i)(-3 + 11i) = 4i$.
- Next, $\dfrac{-3 + 11i}{4i} = \dfrac{11}{4} + \dfrac{3}{4}i$, so rounding to the nearest Gaussian integer yields the quotient $3 + i$, and the remainder is then $(-3 + 11i) - (3 + i)(4i) = 1 - i$.
- Finally, $\dfrac{4i}{1 - i} = -2 + 2i$, so the quotient is $-2 + 2i$ and the remainder is 0.
- The last nonzero remainder is $\boxed{1 - i}$ so it is a gcd. Backsolving yields

$$\begin{aligned} -3 + 11i &= 1 \cdot (9 + 43i) - (1 + i) \cdot (22 + 10i) \\ 4i &= (22 + 10i) - (-2i)\left[1 \cdot (9 + 43i) - (1 + i) \cdot (22 + 10i)\right] \\ &= (3 - 2i) \cdot (22 + 10i) + (2i) \cdot (9 + 43i) \\ 1 - i &= \left[1 \cdot (9 + 43i) - (1 + i) \cdot (22 + 10i)\right] - (3 + i)\left[(3 - 2i) \cdot (22 + 10i) + (2i) \cdot (9 + 43i)\right] \\ &= (3 - 6i) \cdot (9 + 43i) + (-12 + 2i) \cdot (22 + 10i) \end{aligned}$$

  and so we have $1 - i = \boxed{(3 - 6i) \cdot (9 + 43i) + (-12 + 2i) \cdot (22 + 10i)}$.

---

5. 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 $2^{29} - 1 = \boxed{233 \cdot 1103 \cdot 2089}$.

---

6. For all of the factorizations in problem 5, 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, $q \equiv 1 \pmod{p}$.

---

7. The goal of this problem is to prove that the ring $R = \mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain under its norm function $N(a + b\sqrt{-2}) = a^2 + 2b^2$ using a similar argument to the one used to show $\mathbb{Z}[i]$ is Euclidean.

   (a) Suppose that $c + d\sqrt{-2}$ is not zero. Write $\dfrac{a + b\sqrt{-2}}{c + d\sqrt{-2}}$ in the form $x + y\sqrt{-2}$ for rational numbers x and y. [Hint: Rationalize the denominator.]

   - Rationalize the denominator: $\dfrac{a + b\sqrt{-2}}{c + d\sqrt{-2}} = \dfrac{(a + b\sqrt{-2})(c - d\sqrt{-2})}{c^2 + 2d^2} = \dfrac{ac + 2bd}{c^2 + 2d^2} + \dfrac{bc - ad}{c^2 + 2d^2}\sqrt{-2}$.

   (b) With notation from part (a), let s be the closest integer to x and t be the closest integer to y. Set $q = s + t\sqrt{-2}$ and $r = (a + b\sqrt{-2}) - (s + t\sqrt{-2})(c + d\sqrt{-2})$. Prove that $N(r) \leq \dfrac{3}{4}N(c + d\sqrt{-2})$.

   - Note $\dfrac{r}{c + d\sqrt{-2}} = \dfrac{a + b\sqrt{-2}}{c + d\sqrt{-2}} - q = (x - s) + (y - t)\sqrt{-2}$ and that $|x - s| \leq \dfrac{1}{2}$ and $|y - t| \leq \dfrac{1}{2}$.
   - Then $N\left(\dfrac{r}{c + d\sqrt{-2}}\right) = N[(x - s) + (y - t)\sqrt{-2}] = (x - s)^2 + 2(y - t)^2 \leq \dfrac{1}{4} + 2 \cdot \dfrac{1}{4} = \dfrac{3}{4}$.
   - Since N is multiplicative, by rearranging we immediately obtain $N(r) \leq \dfrac{3}{4}N(c + d\sqrt{-2})$ as required.

   (c) Deduce that R is a Euclidean domain.

   - By part (b), N is a norm yielding a division algorithm on R, since the norm of the remainder term is less than the norm of $c + d\sqrt{-2}$.

   (d) Use the Euclidean algorithm in R to find the greatest common divisor of $33 + 5\sqrt{-2}$ and $8 + 11\sqrt{-2}$ in R, and then write the gcd as a linear combination of these elements.

   - First, $\dfrac{33 + 5\sqrt{-2}}{8 + 11\sqrt{-2}} = \dfrac{11}{9} - \dfrac{19}{18}\sqrt{-2}$, so rounding to the nearest element of R yields the quotient $1 - \sqrt{-2}$, and the remainder is then $(33 + 5\sqrt{-2}) - (1 - \sqrt{-2})(8 + 11\sqrt{-2}) = 3 + 2\sqrt{-2}$.
   - Then $\dfrac{8 + 11\sqrt{-2}}{3 + 2\sqrt{-2}} = 4 + \sqrt{-2}$, and so the quotient is $4 + \sqrt{-2}$ and the remainder is 0.
   - The last nonzero remainder is $\boxed{3 + 2\sqrt{-2}}$ so it is a gcd.
   - Backsolving yields $3 + 2\sqrt{-2} = \boxed{1 \cdot (33 + 5\sqrt{-2}) - (1 - \sqrt{-2})(8 + 11\sqrt{-2})}$.

Remark: By a similar argument, one may show that $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are also Euclidean domains.
