Exercise 1. *Show that if* $\gcd(a, c) = 1$*, then* $\gcd(ab, c) = \gcd(b, c)$.

Definition 1. *A set* S *along with a binary operation*[1] $*$ *is an* ***abelian group*** *if there is an element* e *of* S *such that:*

(1) For any $a \in S$*,* $a * e = e * a = a$ *and there exists* $b \in S$ *such that* $a * b = b * a = e$.
(2) For any $a, b \in S$*,* $a * b = b * a$.
(3) For any $a, b, c \in S$*,* $a * (b * c) = (a * b) * c$.

The element e *is called the* ***identity*** *and the element* b *such that* $a * b = e$ *is called the* ***inverse*** *of* a *and written* a^{-1}*. The third property is the associativity of* $*$.

Exercise 2. *Check that the set* $\mathbb{Z}$ *of integers with addition* $+$ *as the binary operation forms an abelian group. (You are allowed to use known properties of* $\mathbb{Z}$*. It is not necessary to axiomatically derive the commutativity and associativity.)*

Exercise 3. *Does the set* $\mathbb{Q}$ *of rational numbers with multiplication* $\cdot$ *as the binary operation form an abelian group? If yes, then prove it. If not, then explain which property is not satisfied. (If yes, you are allowed to use known properties of* $\mathbb{Q}$*. It is not necessary to axiomatically derive the commutativity and associativity.)*

Exercise 4. *(Bonus) The second property for abelian groups describes the* ***commutativity*** *of an abelian group. Removing this condition recovers the definition of a* ***group****.*

There are many groups that do not satisfy the commutativity condition. For example the set of strictly increasing functions from the set $\mathbb{R}$ *of real numbers to* $\mathbb{R}$ *with composition as the binary operation. Write down two such functions* $f(x)$ *and* $g(x)$ *such that* $f(g(x)) \neq g(f(x))$.

[1] A binary operation takes two elements of S and returns one element of S.

Exercise 1. *Prove that for any integer $n \geqslant 1$,*

$$1^3 + 2^3 + \ldots + n^3 = \frac{n^2(n+1)^2}{4}.$$

Exercise 2. *Prove that for any integer $n \geqslant 1$,*

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} \leqslant 2 - \frac{1}{n}.$$

Exercise 3. *Recall the definition of the Fibonacci sequence: $f_1 = f_2 = 1$ and $f_n = f_{n-2} + f_{n-1}$ for any $n \geqslant 3$. Prove that for any integer $n \geqslant 1$,*

$$f_1 + f_3 + f_5 + \ldots f_{2n-1} = f_{2n}.$$

Exercise 4. *(No need to write this down, but please think of it)*

What is wrong with the following argument that all horses look the same? Let $\mathcal{P}(n)$ be the statement that any set of n horses look the same. The base case $\mathcal{P}(1)$ is clearly true. For the induction step, assume that $\mathcal{P}(1), \ldots, \mathcal{P}(n-1)$ are all true. Now take any set of n horses. Removing one horse leaves us with $n-1$ horses which by induction hypothesis all look the same. Now removing a different horse from the original set of n leaves us with another set of $n-1$ horses which by the induction hypothesis all look the same. Therefore, all the horses look the same as there are overlapping $n-2$ horses among the two sets.

Exercise 1. *For any integer n, prove that $3n^7 + 7n^3 + 11n$ is divided by 21.*

Exercise 2. *Let G be a finite abelian group, with binary operation $\cdot$ and identity element e. Let a be an element of G. Prove that $a^{\#G} = e$. Here $a^{\#G}$ means $a \cdot \ldots \cdot a$ (a appears $\#G$-times).*

The last exercise justifies the word "ring".

Definition 1. *A set R along with two binary operations $+$ and $\cdot$ is a **commutative ring** if the following conditions hold:*

(1) $(R, +)$ forms an abelian group. The identity of this group is usually denoted by 0.
(2) For any elements a, b of R, $a \cdot b = b \cdot a$.
(3) For any elements a, b, c of R, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(4) There is an element 1 of R such that $1 \cdot a = a \cdot 1 = a$ for any element a of R.
(5) For any elements a, b, c of R, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Then the set $\mathbb{Z}/m\mathbb{Z}$ of congruence classes modulo m with the addition and the multiplication described in the class is a commutative ring. (This is easy to check)

Exercise 3. *Show that when m is not a prime number, then there exists nonzero elements a, b in $\mathbb{Z}/m\mathbb{Z}$ such that $ab = 0$. Show that when m is a prime number, then there does not exist nonzero elements a, b in $\mathbb{Z}/m\mathbb{Z}$ such that $ab = 0$.*

A nonzero element a of a commutative ring R such that there exists a nonzero element b in R with $a \cdot b = 0$ is called a **zero-divisor**. A commutative ring with no zero-divisors is called an **integral domain**. This exercise is equivalent to saying that $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is a prime number.

Exercise 1. *Prove the following generalization of CRT: Let $a_1, \dots, a_n$ be pairwise coprime positive integers. Let $x_1, \dots, x_n$ be integers. Then there exists a unique congruence class in $\mathbb{Z}/m\mathbb{Z}$, where $m = a_1 \cdots a_n$, such that $x \equiv x_i \pmod{a_i}$ for all $i = 1, \dots, n$. (Hint: Do induction on n.)*

Exercise 2. *Let G and H be two abelian groups with binary operations $*_G$, $*_H$ and the identity elements e_G, e_H. Let $G \times H$ be the set consisting of pairs (a, b) where $a \in G$ and $b \in H$. Define a binary operation $*$ on $G \times H$ by*

$$(a_1, b_1) * (a_2, b_2) = (a_1 *_G a_2, b_1 *_H b_2).$$

Show that $G \times H$ with the binary operation $*$ and the identity element (e_G, e_H) forms an abelian group.

Definition 1. *Let G and H be two abelian groups with binary operations $*_G$, $*_H$ and the identity elements e_G, e_H. A map $f \colon G \to H$ is a **homomorphism** if the following conditions hold:*

(1) $f(e_G) = e_H$,

(2) for any elements a, b of G, we have $f(a *_G b) = f(a) *_H f(b)$.

*A homomorphism f is an **isomorphism**, and we say that G and H are **isomorphic as groups**, if for any element b of H there exists a unique element $a \in G$ with $f(a) = b$.*

In other words, a homomorphism between abelian groups is a map that respects all the group structures, and an isomorphism is a homomorphism that is both injective and surjective.

Exercise 3. *Write down the definition of a homomorphism between two commutative rings. (You only need to write down the definition, no need to check it).*

Remark 4. *Suppose a, b are two coprime positive integers and write $m = ab$. Reducing a congruence class modulo m further modulo a and modulo b gives a map $f \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Then the Chinese Reminder Theorem can be stated as follows: the map f is an isomorphism of commutative rings (meaning that f is a homomorphism between two commutative rings which is both injective and surjective).*

Exercise 1. *Let p be a prime number. Consider the field $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot; [0], [1])$. Prove that $[a] = [a]^{-1}$ if and only if $[a] = [1]$ or $[p-1]$.*

Hint: use $a^2 - 1 = (a+1)(a-1)$ and the fact that $\mathbb{F}_p$ is a field (so $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$).

Exercise 2. *Show that if a and b are two elements of $\mathbb{F}_p$, then $(a+b)^p = a^p + b^p$.*

Exercise 3. *(Bonus) Suppose $f\colon G \to H$ is a map between two finite sets of the same size. Suppose f is injective. That is, if $f(a) = f(b)$ for some $a, b \in G$, then $a = b$. Show that f is surjective. That is, show that for any $b \in H$, there exists some $a \in G$ such that $f(a) = b$.*

The following statement, which is called the **Pigeonhole Principle**, may be useful to prove Exercise 3: if n pigeons are placed in k cages and $n > k$, then there is at least one cage with at least 2 pigeons.

Exercise 1. *Let F be a field. Let $f(x)$ and $g(x)$ be two polynomials in $F[x]$. Show that if* $\deg(f) > \deg(g)$*, then*

$$\deg(f(x) + g(x)) = \deg(f).$$

(An equivalent way to state the result is: $\deg(f(x) + g(x)) = \max\{\deg(f), \deg(g)\}$ *if* $\deg(f) \neq \deg(g)$*.)*

Exercise 2. *Let F be a field. Let $f(x)$ and $g(x)$ be two polynomials in $F[x]$. Show that if* $\deg(f) \geq \deg(g)$*, then*

$$\deg(f(x) + g(x)) \leq \deg(f).$$

(An equivalent way to state the result is: $\deg(f(x) + g(x)) \leq \max\{\deg(f), \deg(g)\}$*.)*

Exercise 3. *For any polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_p[x]$, show that $f(x)^p = \sum_{i=0}^{n} a_i x^{ip}$. (Hint: do Induction on* $\deg(f)$ *when $f \neq 0$.)*

Exercise 4. *Show that if $f(x)$ and $g(x)$ are two polynomials in $\mathbb{F}_p[x]$, then $(f(x) + g(x))^p = f(x)^p + g(x)^p$. (Hint: Use Exercise 2 from last time and Exercise 3.)*

Exercise 1. *Let F be a field. Let $f_1(x), f_2(x), \ldots, f_n(x) \in F[x]$ be pairwise coprime polynomials, namely there are no irreducible polynomials dividing both $f_i(x)$ and $f_j(x)$ for any $i \neq j$. Prove: if $g(x) \in F[x]$ satisfies $f_i(x)|g(x)$ for any $i \in \{1, \ldots, n\}$, then $f_1(x)f_2(x)\cdots f_n(x)|g(x)$.*

Exercise 2. *Prove the following generalization of Proposition 7.12: Let F be a field. Let $f(x)$ and $g(x)$ be polynomials in $F[x]$. Suppose that $g(x)$ is irreducible and that $g'(x)$ is nonzero. Suppose r is a positive integer such that $\mathrm{char}(F) \nmid r$. Then $g(x)^{r+1}$ divides $f(x)$ if and only if $g(x)^r$ divides $\gcd(f(x), f'(x))$.*

Exercise 3. *Let F be a field. Let $f(x) \in F[x]$ non-constant such that $\gcd(f(x), f'(x)) = 1$ (in particular $f'(x) \neq 0$). Prove that all roots of $f(x)$ in F are distinct.*

Exercise 4. *For any prime number p and positive integer r, show that*

$$f(x_0 + p^r a) \equiv f(x_0) + f'(x_0)p^r a \pmod{p^{r+1}}$$

for any $f(x) \in \mathbb{Z}[x]$.

In principle, these problems can already be solved after the class of October 10.

In what follows, F will always be a field. For any nonzero polynomial $f(x) \in F[x]$, define its **radical**, denoted by $\mathrm{rad}(f)$, as the product the all monic irreducible factors of $f(x)$. For example, for $(x^2+1)^3x^2(2x-1) \in \mathbb{Q}[x]$, we have

$$\mathrm{rad}((x^2+1)^3x^2(2x-1)) = (x^2+1)x(x-\frac{1}{2}).$$

In general if $f(x) = cp_1(x)^{\alpha_1}\cdots p_n(x)^{\alpha_n}$ where $c \in F^\times$, the $p_i(x)$'s are monic irreducible polynomials and the α_i's are positive integers (the Unique Factorization Theorem tells us that this expression is unique), then $\mathrm{rad}(f) = p_1(x)\cdots p_n(x)$.

Exercise 1. *For any non-constant polynomial $f(x) \in \mathbb{Q}[x]$ with $f(x) = cp_1(x)^{\alpha_1}\cdots p_n(x)^{\alpha_n}$ as the factorization into monic irreducible polynomials as above, prove* $\deg(f) - \deg(\mathrm{rad}(f)) \leq \deg(\gcd(f(x), f'(x)))$. *(Hint: prove $p_1(x)^{\alpha_1-1}\cdots p_n(x)^{\alpha_n-1} | \gcd(f(x), f'(x))$.)*

Exercise 2. *(Mason's Theorem). Let $f(x)$, $g(x)$ and $h(x)$ be non-constant polynomials in $\mathbb{Q}[x]$ such that no irreducible polynomial divides all three of them. Suppose $f(x)+g(x) = h(x)$. We prove the following inequality:*

$$\max\{\deg(f), \deg(g), \deg(h)\} \leq \deg(\mathrm{rad}(f(x)g(x)h(x))) - 1.$$

(1) Prove that f, g and h are pairwise coprime (namely any two of f, g and h are coprime). Deduce that $\gcd(f, f')$, $\gcd(g, g')$ *and* $\gcd(h, h')$ *are pairwise coprime.*

(2) Prove: $f'(x)g(x) - g'(x)f(x) = f'(x)h(x) - h'(x)f(x)$. Deduce that $\gcd(f, f')$, $\gcd(g, g')$ *and* $\gcd(h, h')$ *all divide $f'(x)g(x) - g'(x)f(x)$.*

(3) Prove: $\gcd(f, f')\gcd(g, g')\gcd(h, h') | f'(x)g(x) - g'(x)f(x)$.

(4) Prove the following inequalities:

$$\begin{aligned}
&\deg(f) + \deg(g) + \deg(h) - \deg(\mathrm{rad}(f)) - \deg(\mathrm{rad}(g)) - \deg(\mathrm{rad}(h)) \\
\leq &\deg(f'(x)g(x) - g'(x)f(x)) \\
\leq &\deg(f) + \deg(g) - 1.
\end{aligned}$$

(5) Prove:

$$\begin{aligned}
&\deg(h) \\
\leq &\deg(\mathrm{rad}(f)) + \deg(\mathrm{rad}(g)) + \deg(\mathrm{rad}(h)) - 1 \\
= &\deg(\mathrm{rad}(f)\mathrm{rad}(g)\mathrm{rad}(h)) - 1 \\
= &\deg(\mathrm{rad}(fgh)) - 1.
\end{aligned}$$

(6) Conclude by rewriting the equation $f+g=h$ as $f+(-h) = -g$ (so that "$g(x)$" becomes "$-h(x)$" and "$h(x)$" becomes "$-g(x)$") and $g+(-h) = -f$. Your argument for this question should not exceed four lines.

Exercise 3. *Formulate the analogous statement of Mason's Theorem, namely Exercise 2, for $\mathbb{Z}$ (i.e. replace $\mathbb{Q}[x]$ by $\mathbb{Z}$). This statement is called the abc conjecture. (Hint: start by defining the radical for any integer). You only need to write down this statement and no explanation or proof is required.*

Exercise 4. *The goal of this exercise is to prove the following result (known as Fermat's Last Theorem for $\mathbb{Q}[x]$): Let $n \geq 3$ be an integer. Then there are no non-constant polynomials $f(x)$, $g(x)$ and $h(x)$ in $\mathbb{Q}[x]$ such that there is no irreducible polynomial dividing all three of them and they satisfy*

$$f(x)^n + g(x)^n = h(x)^n.$$

(Hint: apply Mason's Theorem, namely Exercise 3, to $f(x)^n$, $g(x)^n$ and $h(x)^n$).

Exercise 5. *Formulate the analogue of Fermet's Last Theorem for $\mathbb{Q}[x]$, namely Exercise 4, for $\mathbb{Z}$ (i.e. replace $\mathbb{Q}[x]$ by $\mathbb{Z}$). This statement is called Fermat's Last Theorem. You only need to write down this statement and no explanation or proof is required.*

A bonus will be given if you use the abc conjecture, namely the statement that you formulated in Exercise 3, to prove Fermat's Last Theorem for $\mathbb{Z}$.

Exercise 6. *(Bonus) Briefly explain why our statements for Mason's Theorem and Fermat's Last Theorem for $\mathbb{Q}[x]$ are wrong when $\mathbb{Q}[x]$ is replaced by $\mathbb{F}_p[x]$. You can do this either by pointing out which step of your proof does not work for $\mathbb{F}_p[x]$ or by giving a counterexample. A bonus will be given if you can furthermore correct the statements for $\mathbb{F}_p[x]$ (no need to prove this correction).*

Exercise 1. *Let $(G, \cdot; e)$ be an abelian group and let a be an element of G. Suppose $m \neq 0$ is an integer. Prove that the order of a^m is $\mathrm{ord}(a)/\gcd(m, \mathrm{ord}(a))$ if $\mathrm{ord}(a) < +\infty$ and is $+\infty$ if $\mathrm{ord}(a) = +\infty$.*

Exercise 2. *Let G be an abelian group such that $\#G = n$. Prove that the order of any element $a \in G$ divides n. (Hint: note that $\mathrm{ord}(e) = 1$).*

Exercise 3. *Let F be a field of characteristic p. Let $q = p^r$ for some positive integer r. Prove that $(a + b)^q = a^q + b^q$ for any $a, b \in F$.*

Exercise 1. *Let F be a finite field with $\mathrm{char}(F) = p$. Prove that every element is a p-th power, namely for any $a \in F$, there exists $b \in F$ such that $a = b^p$.*

Exercise 2. *Let F be an algebraically closed field of characteristic p and let n be a positive integer such that $\gcd(p, n) = 1$. We prove that there exists a primitive n-th root of unity in F, namely an element $a \in F$ such that $\mathrm{ord}(a) = n$ in the group $(F^\times, \cdot; 1_F)$, following the steps:*

(1) Prove that this is true when $n = l^m$ for any prime number $l \neq p$. (Hint: use induction on m).

(2) Prove it for any n by the Unique Factorization Theorem.

Exercise 3. *Let p be a prime number and let $q = p^m$ for some positive integer m. Let a be a primitive $(q-1)$-th root of unity in $\overline{\mathbb{F}}_p$. Prove that $a \in \mathbb{F}_q$.*

Exercise 4. *Prove the following statement: For any prime number p and any positive integer m, the field $\mathbb{F}_{p^m}$ has a primitive $(p^m - 1)$-th root of unity (namely an element $a \in \mathbb{F}_{p^m}$ such that $\mathrm{ord}(a) = p^m - 1$ in the group $(\mathbb{F}_{p^m}^\times, \cdot; 1)$).*

Exercise 1. *Let p be a prime number and let $q = p^m$ for some positive integer m. Show that the number of squares in $\mathbb{F}_q$ is q is $p = 2$; and is $\frac{q+1}{2}$ if $p > 2$.*

Exercise 2. *Suppose p is a prime number congruent to 3 modulo 4, so that $(p+1)/4 \in \mathbb{Z}$. Assume that a is a quadratic residue modulo p. Prove that $a^{(p+1)/4}$ is a solution to the equation $x^2 \equiv a \pmod{p}$.*

Exercise 3. *Suppose a is an odd integer. Show that if the equation $x^2 \equiv a \pmod{8}$ has a solution, then the equation $x^2 \equiv a \pmod{2^n}$ has solutions for every $n \geq 3$. (Hint: Modify the proof of Hensel's Lemma.)*

Exercise 4. *Prove that if r is a quadratic residue modulo $m > 2$ and $\gcd(r, m) = 1$, then $r^{\phi(m)/2} \equiv 1 \pmod{m}$.*

Exercise 5. *Let $p > 2$ be a prime number. Prove that any quadratic residue modulo p are congruent to one of 1^2, 2^2, ..., $(\frac{p-1}{2})^2$.*

Exercise 6. *Let $p > 3$ be a prime number. Prove that the sum of the quadratic residues is divisible by p.*

In this homework, we will apply the same technique used in class to understand what integers can be written in the form $x^2 + 2y^2$ for integers x, y. The proof is parallel to what we did (or will do on Thursday) in class.

The conclusion is the following statement:

Theorem 1. *A positive integer m is expressible as $x^2 + 2y^2$ where x, y are integers if and only if when $m = 2^\alpha p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ is written as a product of primes, the exponent α_i is even if $p_i \equiv 5, 7 \pmod 8$.*

Exercise 1. *Suppose p is an odd prime number. Show that the equation $x^2 + 2y^2 \equiv 0 \pmod p$ has nontrivial solutions (meaning p does not divide x or y) if and only if $p \equiv 1, 3 \pmod 8$.*

Next we need some kine of "composition law" similar to equation (1) we wrote in class to know that the product of two integers expressible as $x^2 + 2y^2$ is also expressible as $x^2 + 2y^2$. That is, we need a formula of the form:

$$(x^2 + 2y^2)(u^2 + 2v^2) = ()^2 + 2()^2. \tag{0.1}$$

Of course we can try to be smart and just write one down, or we can do it systematically by studying the ring $\mathbb{Z}[\sqrt{-2}]$ (see Exercise 3 below). Just like $\mathbb{Z}[i]$, we let $\sqrt{-2}$ denote a root of $x^2 + 2$ in $\mathbb{C}$, and then as a set $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} | a, b \in \mathbb{Z}\}$.

Exercise 2. *Write down the addition and multiplication formula for $\mathbb{Z}[\sqrt{-2}]$.*

With your addition and multiplication formula, $(\mathbb{Z}[\sqrt{-2}], +, \cdot; 0, 1)$ is a commutative ring. The multiplication formula you write down should tell you how to complete the equation (0.1) above. We define the **norm** of an element $\alpha = a + b\sqrt{-2}$ to be $N(\alpha) = (a + b\sqrt{-2})(a - b\sqrt{-2}) = a^2 + 2b^2$ (do not confuse with the norm for $\mathbb{Z}[i]$).

Exercise 3. *Complete equation (0.1). This should correspond to $N(\alpha\beta) = N(\alpha)N(\beta)$ for any $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$.*

Exercise 4. *(Invertible Elements) Prove that $\mathbb{Z}[\sqrt{-2}]^\times = \{1, -1\}$.*

Exercise 5. *(Division Algorithm) Show that for any $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ with $\beta \neq 0$, there exist elements $\gamma, \delta \in \mathbb{Z}[\sqrt{-2}]$ such that*

$$\alpha = \beta\gamma + \delta, \qquad \text{with } N(\delta) < N(\beta).$$

Exercise 6. *Conclude Theorem 1:*

1. *Use Exercise 1 to prove the neccessicity (i.e. $\Rightarrow$).*
2. *Use equation (0.1) to translate the sufficiency (i.e. $\Leftarrow$) to: if p is a prime number congruent to 1 or 3 modulo 8, then p is expressible as $x^2 + 2y^2$.*
3. *Conclude.*

Exercise 1. *Write down two equivalent definitions for prime elements in* $\mathbb{Z}[\sqrt{-2}]$. *Prove their equivalence.*

Exercise 2. *Write down the UFT for* $\mathbb{Z}[\sqrt{-2}]$. *No need to prove it.*[1]

Exercise 3. *Give a classification of prime elements of* $\mathbb{Z}[\sqrt{-2}]$ *similar to Theorem 16.9. Prove this classification.*

[1]This UFT is true because of the existence of gcd!

Exercise 1. *Show that if r, s are coprime positive integers such that rs is a square, then $r = r_1^2$ and $s = s_1^2$ for some integers r_1, s_1.*

Exercise 2. *Find all integer solutions to $x^2 + y^2 = 2z^2$. (Hint: consider $(x+y)^2 + (x-y)^2$)*

Exercise 3. *Find all integer solutions to $x^4 - 2y^2 = 1$.*

Exercise 4. *Show that neither of the equations $x^4 + 4y^4 = z^2$ and $x^4 + y^2 = z^4$ has a solution in positive integers.*

Exercise 5. *Show that there exist no positive integers m and n such that $m^2 + n^2$ and $m^2 - n^2$ are both squares.*

Exercise 6. *Consider a right angle triangle, the lengths of whose sides are integers. Prove that the area cannot be a square.*

Exercise 1. *Prove that the equation* $x^2 + 2y^2 = 8z + 5$ *has no integer solutions.*

Exercise 2. *Show that any cube mod* 7 *is* 0 *or* ± 1. *Use this to deduce that the only integer solution to* $x^3 + 2y^3 = 7(z^3 + 2w^3)$ *is* $(0, 0, 0, 0)$.

Exercise 3. *Show that the equation* $y^2 = x^3 + 23$ *has no integer solutions.*

Exercise 4. *Find all integer solutions to* $x^4 + 2x^3 + 2x^2 + 2x + 5 = y^2$.