A Tour of Joseph-Louis Lagrange's *Recherches d'Arithmetique*

Erik R. Tou

School of Interdisciplinary Arts & Sciences
University of Washington, Tacoma

Binary Quadratic Forms

Definition

A *binary quadratic form* is a homogeneous polynomial with two variables:

$$ax^2 + bxy + cy^2,$$

where a, b, c are integers. Its *discriminant* is defined as $\Delta = b^2 - 4ac$.

Binary Quadratic Forms

Definition

A *binary quadratic form* is a homogeneous polynomial with two variables:

$$ax^2 + bxy + cy^2,$$

where a, b, c are integers. Its *discriminant* is defined as $\Delta = b^2 - 4ac$.

Definition

A form *represents* an integer τ if there are integer values of x, y for which $\tau = ax^2 + bxy + cy^2$. The representation is *primitive* if $\gcd(x, y) = 1$. We then say τ is *representable* (or, *primitively representable*) by the form.

Classic Questions: What integers can be represented by a given form? What forms can represent a given integer?

Fermat and Euler

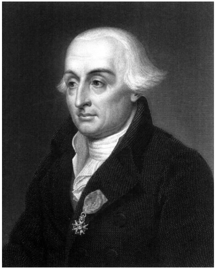
Pierre de Fermat (1607-1665) conjectured that every prime p of the form $4n+1$ can be represented uniquely as the sum of two squares. Leonhard Euler (1707-1783) proved this result in 1749.

> 2. Sur le sujet des triangles rectangles ('), voici mes fondements :
>
> 1° Tout nombre premier, qui surpasse de l'unité un multiple du quaternaire, est une seule fois la somme de deux quarrés, et une seule fois l'hypoténuse d'un triangle rectangle.
>
> 2° Le même nombre et son quarré sont chacun une fois la somme de deux quarrés ;

Figure: A letter from Fermat to Marin Mersenne, 25 December 1640.

Joseph-Louis Lagrange

A frequent correspondent of Euler's, Joseph-Louis Lagrange (1736-1813) took up Euler's vacant chair in Berlin when Euler left the Berlin Academy to return to Russia.



While in Berlin, Lagrange built upon Euler's earlier contributions to the study of Diophantine equations.

Recherches d'Arithmétique

From the *Nouveaux Mémoires* of the Berlin Academy, 1775:

RECHERCHES D'ARITHMÉTIQUE.

PAR M. DE LA GRANGE.

Ces recherches ont pour objet les nombres qui peuvent être repréſentés par la formule $Bt^2 + Ctu + Du^2$, où B, C, D ſont ſuppoſés des nombres entiers donnés, & t, u des nombres auſſi entiers mais indéterminés. Je donnerai d'abord la maniere de trouver toutes les diffé-

"This research has for its object the numbers which may be represented by the formula $Bt^2+Ctu+Du^2$, where B, C, D are assumed to be given whole numbers, and t, u are also whole (though variable) numbers."

Recherches d'Arithmétique

Lagrange's plan of attack:

- "First, I will give the manner by which to find all the different forms whose **divisors** are the kind of numbers that are susceptible [to this representation].

Recherches d'Arithmétique

Lagrange's plan of attack:

- "First, I will give the manner by which to find all the different forms whose **divisors** are the kind of numbers that are susceptible [to this representation].
- Next, I will give a method for **reducing these forms** to the smallest number possible...

Recherches d'Arithmétique

Lagrange's plan of attack:

- "First, I will give the manner by which to find all the different forms whose **divisors** are the kind of numbers that are susceptible [to this representation].
- Next, I will give a method for **reducing these forms** to the smallest number possible...
- Finally, I will prove several Theorems on **prime numbers** of the same form $Bt^2 + Ctu + Du^2$, of which some are already known, but have not yet been proven, and of which others are entirely new."

Recherches d'Arithmétique

Theorem (I)

If the number A is a divisor of a number primitively represented by $Bt^2 + Ctu + Du^2$, then A is primitively representable by some form $Ls^2 + Msx + Nx^2$, where $4LN - M^2 = 4BD - C^2 = -\Delta$.

Recherches d'Arithmétique

Theorem (I)

If the number A is a divisor of a number primitively represented by $Bt^2 + Ctu + Du^2$, then A is primitively representable by some form $Ls^2 + Msx + Nx^2$, where $4LN - M^2 = 4BD - C^2 = -\Delta$.

Theorem (II)

Every quadratic form $Ls^2 + Msx + Nx^2$ for which $|M| > |L|$ or $|N|$ may be transformed into a form $L's'^2 + M's'x' + N'x'^2$ with the same discriminant Δ, where $|M'| < |M|$.

Recherches d'Arithmétique

Theorem (I)

If the number A is a divisor of a number primitively represented by $Bt^2 + Ctu + Du^2$, then A is primitively representable by some form $Ls^2 + Msx + Nx^2$, where $4LN - M^2 = 4BD - C^2 = -\Delta$.

Theorem (II)

Every quadratic form $Ls^2 + Msx + Nx^2$ for which $|M| > |L|$ or $|N|$ may be transformed into a form $L's'^2 + M's'x' + N'x'^2$ with the same discriminant Δ, where $|M'| < |M|$.

Example. Given that 425 is primitively representable by $t^2 + 2tu + 2u^2$, determine the forms that its divisor 85 can have.

An Example of Theorem I

Quadratic Form: $425 = t^2 + 2tu + 2u^2 = 11^2 + 2(11)(-19) + 2(-19)^2$

Linear Form: $t = 1u + 5x = 1(-19) + 5(6) = 11$

An Example of Theorem I

Quadratic Form: $425 = t^2 + 2tu + 2u^2 = 11^2 + 2(11)(-19) + 2(-19)^2$

Linear Form: $t = 1u + 5x = 1(-19) + 5(6) = 11$

Number	$=$	t^2 term	$+$	tu term	$+$	u^2 term
425	$=$	$1t^2$	$+$	$2tu$	$+$	$2u^2$

An Example of Theorem I

Quadratic Form: $425 = t^2 + 2tu + 2u^2 = 11^2 + 2(11)(-19) + 2(-19)^2$

Linear Form: $t = 1u + 5x = 1(-19) + 5(6) = 11$

Number	=	t^2 term	+	tu term	+	u^2 term
425	=	$1t^2$	+	$2tu$	+	$2u^2$
425	=	$1(1u+5x)^2$	+	$2(1u+5x)u$	+	$2u^2$

An Example of Theorem I

Quadratic Form: $425 = t^2 + 2tu + 2u^2 = 11^2 + 2(11)(-19) + 2(-19)^2$

Linear Form: $t = 1u + 5x = 1(-19) + 5(6) = 11$

Number	=	t^2 term	+	tu term	+	u^2 term
425	=	$1t^2$	+	$2tu$	+	$2u^2$
425	=	$1(1u + 5x)^2$	+	$2(1u + 5x)u$	+	$2u^2$
425	=	$(1 + 2 + 2)u^2$	+	$(10 + 10)ux$	+	$25x^2$

An Example of Theorem I

Quadratic Form: $425 = t^2 + 2tu + 2u^2 = 11^2 + 2(11)(-19) + 2(-19)^2$

Linear Form: $t = 1u + 5x = 1(-19) + 5(6) = 11$

Number	=	t^2 term	+	tu term	+	u^2 term
425	=	$1t^2$	+	$2tu$	+	$2u^2$
425	=	$1(1u+5x)^2$	+	$2(1u+5x)u$	+	$2u^2$
425	=	$(1+2+2)u^2$	+	$(10+10)ux$	+	$25x^2$
Number	=	s^2 term	+	sx term	+	x^2 term
425	=	$5s^2$	+	$20sx$	+	$25x^2$

An Example of Theorem I

Quadratic Form: $425 = t^2 + 2tu + 2u^2 = 11^2 + 2(11)(-19) + 2(-19)^2$

Linear Form: $t = 1u + 5x = 1(-19) + 5(6) = 11$

Number	$=$	t^2 term	$+$	tu term	$+$	u^2 term
425	$=$	$1t^2$	$+$	$2tu$	$+$	$2u^2$
425	$=$	$1(1u+5x)^2$	$+$	$2(1u+5x)u$	$+$	$2u^2$
425	$=$	$(1+2+2)u^2$	$+$	$(10+10)ux$	$+$	$25x^2$
Number	$=$	s^2 term	$+$	sx term	$+$	x^2 term
425	$=$	$5s^2$	$+$	$20sx$	$+$	$25x^2$
85	$=$	$1s^2$	$+$	$4sx$	$+$	$5x^2$

An Example of Theorem I

Quadratic Form: $425 = t^2 + 2tu + 2u^2 = 11^2 + 2(11)(-19) + 2(-19)^2$

Linear Form: $t = 1u + 5x = 1(-19) + 5(6) = 11$

Number	=	t^2 term	+	tu term	+	u^2 term
425	=	$1t^2$	+	$2tu$	+	$2u^2$
425	=	$1(1u+5x)^2$	+	$2(1u+5x)u$	+	$2u^2$
425	=	$(1+2+2)u^2$	+	$(10+10)ux$	+	$25x^2$
Number	=	s^2 term	+	sx term	+	x^2 term
425	=	$5s^2$	+	$20sx$	+	$25x^2$
85	=	$1s^2$	+	$4sx$	+	$5x^2$

Conclusion: $85 = s^2 + 4sx + 5x^2 = (-8)^2 + 4(-8)(7) + 5(7)^2$.

An Example of Theorem II

Quadratic Form: $85 = s^2 + 4sx + 5x^2 = (-8)^2 + 4(-8)(7) + 5(7)^2$

Linear Form: $s = -2x + s' = -2(7) + 6 = -8$

An Example of Theorem II

Quadratic Form: $85 = s^2 + 4sx + 5x^2 = (-8)^2 + 4(-8)(7) + 5(7)^2$

Linear Form: $s = -2x + s' = -2(7) + 6 = -8$

Number	=	s^2 term	+	sx term	+	x^2 term
85	=	$1s^2$	+	$4sx$	+	$5x^2$

An Example of Theorem II

Quadratic Form: $85 = s^2 + 4sx + 5x^2 = (-8)^2 + 4(-8)(7) + 5(7)^2$

Linear Form: $s = -2x + s' = -2(7) + 6 = -8$

Number	=	s^2 term	+	sx term	+	x^2 term
85	=	$1s^2$	+	$4sx$	+	$5x^2$
85	=	$1(-2x+s')^2$	+	$4(-2x+s')x$	+	$5x^2$

An Example of Theorem II

Quadratic Form: $85 = s^2 + 4sx + 5x^2 = (-8)^2 + 4(-8)(7) + 5(7)^2$

Linear Form: $s = -2x + s' = -2(7) + 6 = -8$

Number	=	s^2 term	+	sx term	+	x^2 term
85	=	$1s^2$	+	$4sx$	+	$5x^2$
85	=	$1(-2x + s')^2$	+	$4(-2x + s')x$	+	$5x^2$
85	=	$1s'^2$	+	$(-4 + 4)s'x$	+	$(4 - 8 + 5)x^2$

An Example of Theorem II

Quadratic Form: $85 = s^2 + 4sx + 5x^2 = (-8)^2 + 4(-8)(7) + 5(7)^2$

Linear Form: $s = -2x + s' = -2(7) + 6 = -8$

Number	=	s^2 term	+	sx term	+	x^2 term
85	=	$1s^2$	+	$4sx$	+	$5x^2$
85	=	$1(-2x + s')^2$	+	$4(-2x + s')x$	+	$5x^2$
85	=	$1s'^2$	+	$(-4 + 4)s'x$	+	$(4 - 8 + 5)x^2$
Number	=	s'^2 term	+	$s'x'$ term	+	x'^2 term

An Example of Theorem II

Quadratic Form: $85 = s^2 + 4sx + 5x^2 = (-8)^2 + 4(-8)(7) + 5(7)^2$

Linear Form: $s = -2x + s' = -2(7) + 6 = -8$

Number	$=$	s^2 term	$+$	sx term	$+$	x^2 term
85	$=$	$1s^2$	$+$	$4sx$	$+$	$5x^2$
85	$=$	$1(-2x+s')^2$	$+$	$4(-2x+s')x$	$+$	$5x^2$
85	$=$	$1s'^2$	$+$	$(-4+4)s'x$	$+$	$(4-8+5)x^2$
Number	$=$	s'^2 term	$+$	$s'x'$ term	$+$	x'^2 term
85	$=$	$1s'^2$	$+$	$0s'x'$	$+$	$1x'^2$

An Example of Theorem II

Quadratic Form: $85 = s^2 + 4sx + 5x^2 = (-8)^2 + 4(-8)(7) + 5(7)^2$

Linear Form: $s = -2x + s' = -2(7) + 6 = -8$

Number	$=$	s^2 term	$+$	sx term	$+$	x^2 term
85	$=$	$1s^2$	$+$	$4sx$	$+$	$5x^2$
85	$=$	$1(-2x+s')^2$	$+$	$4(-2x+s')x$	$+$	$5x^2$
85	$=$	$1s'^2$	$+$	$(-4+4)s'x$	$+$	$(4-8+5)x^2$
Number	$=$	s'^2 term	$+$	$s'x'$ term	$+$	x'^2 term
85	$=$	$1s'^2$	$+$	$0s'x'$	$+$	$1x'^2$

Conclusion: $85 = s'^2 + x'^2 = 6^2 + 7^2$.

Recherches d'Arithmétique

Theorem (III)

If A divides a number of the form $Bt^2 + Ctu + Du^2$, it must have the form $Py^2 + Qyz + Rz^2$, where $4PR - Q^2 = 4BD - C^2$ and $|Q| \leq |P|, |R|$.

Corollary (I)

If $4BD - C^2$ is positive, then $Q \leq \sqrt{\frac{4BD-C^2}{3}}$.

Recherches d'Arithmétique

Theorem (III)

If A divides a number of the form $Bt^2 + Ctu + Du^2$, it must have the form $Py^2 + Qyz + Rz^2$, where $4PR - Q^2 = 4BD - C^2$ and $|Q| \leq |P|, |R|$.

Corollary (I)

If $4BD - C^2$ is positive, then $Q \leq \sqrt{\frac{4BD - C^2}{3}}$.

So, "... divisors of the numbers of the form $t^2 + u^2$ are necessarily contained in the formula $y^2 + z^2$, which is to say that every divisor of a number equal to the sum of two squares is also the sum of two squares."

Getting Down To Business

1. "… divisors of the numbers of the form $t^2 + u^2$ are necessarily contained in the formula $y^2 + z^2$, which is to say that every divisor of a number equal to the sum of two squares is also the sum of two squares."
2. "… divisors of the numbers of the form $t^2 + 2u^2$ are contained in the formula $y^2 + 2z^2$."

Getting Down To Business

1. "… divisors of the numbers of the form $t^2 + u^2$ are necessarily contained in the formula $y^2 + z^2$, which is to say that every divisor of a number equal to the sum of two squares is also the sum of two squares."
2. "… divisors of the numbers of the form $t^2 + 2u^2$ are contained in the formula $y^2 + 2z^2$."
3. "… divisors of the numbers of the form $t^2 + 3u^2$ will be contained in the two formulas $y^2 + 3z^2$ and $2y^2 \pm 2yz + 2z^2$."
4. …

Getting Down To Business

1. "... divisors of the numbers of the form $t^2 + u^2$ are necessarily contained in the formula $y^2 + z^2$, which is to say that every divisor of a number equal to the sum of two squares is also the sum of two squares."
2. "... divisors of the numbers of the form $t^2 + 2u^2$ are contained in the formula $y^2 + 2z^2$."
3. "... divisors of the numbers of the form $t^2 + 3u^2$ will be contained in the two formulas $y^2 + 3z^2$ and $2y^2 \pm 2yz + 2z^2$."
4. ...
5. "... odd divisors of the numbers of the form $t^2 + 12u^2$ will be of one or the other of the forms $y^2 + 12z^2$ or $3y^2 + 4z^2$."

Getting Down To Business

TABLE I.

Formule des nombres propofés

$$t^2 + au^2.$$

Formule de leurs divifeurs impairs

$$py^2 \pm 2qyz + rz^2, \quad \text{où } pr - q^2 = a.$$

Valeurs de a	Valeurs correfpondantes de p	q	r
1	1	0	1
2	1	0	2
3	1	0	3
5	1, 2	0, 1	5, 3
6	1, 2	0, 0	6, 3
7	1	0	7
10	1, 2	0, 0	10, 5
11	1, 3	0, 1	11, 4

Getting Down To Business

Valeurs de a	Valeurs correſpondantes de p	q	r
1	1	0	1
2	1	0	2
3	1	0	3
5	1, 2	0, 1	5, 3
6	1, 2	0, 0	6, 3
7	1	0	7
10	1, 2	0, 0	10, 5
11	1, 3	0, 1	11, 4
13	1, 2	0, 1	13, 7
14	1, 2, 3	0, 0, 1	14, 7, 5
15	1, 3	0, 0	15, 5
17	1, 2, 3	0, 1, 1	17, 9, 6
19	1, 4	0, 1	19, 5
21	1, 3, 2, 5	0, 0, 1, 2	21, 7, 11, 5
22	1, 2	0, 0	22, 11
23	1, 3	0, 1	23, 8
26	1, 2, 3, 5	0, 0, 1, 2	26, 13, 9, 6
29	1, 3, 5	0, 1, 1	29, 10, 6
30	1, 3, 5, 2	0, 0, 0, 1	30, 10, 6, 17
31	1, 5	0, 2	31, 7

Coda: Squares in the Year $1801 = 24^2 + 35^2$

Theorem

A number $\tau > 1$ is representable as a sum of two squares, if, and only if, its prime decomposition contains no primes of the form $4n + 3$ raised to an odd power.

Examples:

1. $\tau = 1801 = 24^2 + 35^2$, (primitively) representable.
2. $\tau = 16209 = 1801 \cdot 3^2 = (24^2 + 35^2) \cdot 3^2 = 72^2 + 105^2$, representable.
3. $\tau = 48627 = 1801 \cdot 3^3 = (1801 \cdot 3^2) \cdot 3$, not representable.

Coda: Squares in the Year $1801 = 24^2 + 35^2$

Theorem

A number $\tau > 1$ is representable as a sum of two squares, if, and only if, its prime decomposition contains no primes of the form $4n+3$ raised to an odd power.

Examples:

1. $\tau = 1801 = 24^2 + 35^2$, (primitively) representable.
2. $\tau = 16209 = 1801 \cdot 3^2 = (24^2 + 35^2) \cdot 3^2 = 72^2 + 105^2$, representable.
3. $\tau = 48627 = 1801 \cdot 3^3 = (1801 \cdot 3^2) \cdot 3$, not representable.

Theorem (Gauss, 1801)

A number $\tau > 1$ is primitively representable by the form $t^2 + u^2$, if, and only if, -1 is a quadratic residue modulo τ.

Thank You!

Fermat, Pierre. Letter to Marin Mersenne, 25 December 1640. Appears in: Henry, Charles, *Oeuvres de Fermat: Correspondance*, vol. 2, Gauthier-Villars et fils, 1894.

Gauss, Carl. *Disquisitiones Arithmeticae*. Leipzig: Fleischer, 1801.

Lagrange, Joseph-Louis. "Recherches d'Arithmétique," *Nouveaux Mémoires de l'académie des sciences de Berlin* **5** 1773 (1775), 265-312.

Slides of this presentation available via:
https://tinyurl.com/TouLagrange2022

English translation of Recherches d'Arithmétique at:
https://tinyurl.com/RecherchesdArithmetique