Divisibility Sequences and Diophantine Equations

Jonathan Reynolds

May 7, 2012
Divisibility sequence:

A sequence \((W_m)\) of integers such that \(W_n \mid W_m\) whenever \(n \mid m\).
Divisibility sequence:

A sequence \((W_m)\) of integers such that \(W_n \mid W_m\) whenever \(n \mid m\).

- Natural numbers 1, 2, 3, ..., 
- Fibonacci sequence,
- Mersenne sequence,
- any Lucas sequence.
A large class of divisibility sequences (including the ones already mentioned) can be generated from a Weierstrass equation

\[ C : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \]

with integer coefficients \( a_i \).
A large class of divisibility sequences (including the ones already mentioned) can be generated from a Weierstrass equation

\[ C : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \]

with integer coefficients \(a_i\). The non-singular rational points on \(C\) form a group!
A large class of divisibility sequences (including the ones already mentioned) can be generated from a Weierstrass equation

\[ C : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \]

with integer coefficients \(a_i\). The non-singular rational points on \(C\) form a group! Using the group law, for a non-singular non-torsion point \(P\) on \(C\) with rational coordinates we can write

\[ x(mp) = A_m / B_m^2 \quad \text{and} \quad y(mp) = C_m / B_m^3 \]

in lowest terms (\(A_m, B_m, C_m \in \mathbb{Z}, \gcd(A_mC_m, B_m) = 1\)).
Moreover, for all $n, m \in \mathbb{N}$, if $p \mid B_n$ is a prime then

$$\text{ord}_p(B_{mn}) = \text{ord}_p(B_n) + \text{ord}_p(m)$$

if $a_2$ is even or $p$ is odd, and $\text{ord}_2(B_{mn}) = \text{ord}_2(B_n) + O(1)$.

In particular, the sequence $(B_m)_{m \geq 1}$ of denominators is a divisibility sequence ($n \mid m \implies B_n \mid B_m$).
Integers: Take $P = (0, 0)$ on $C : y^2 + 2xy + 2y = x^3 + 2x^2 + x$ and write $x(mP) = A_m/B_m^2$, then $B_m = m$ for all $m \geq 1$. 

Fibonacci: Take $P = (0, 0)$ on $C : y^2 + xy + y = x^3 - 2x^2 - x$ and write $x(mP) = A_m/B_m^2$, then $(B_m)$ is the Fibonacci sequence.
Integers: Take $P = (0, 0)$ on $C: y^2 + 2xy + 2y = x^3 + 2x^2 + x$ and write $x(mP) = A_m/B_m^2$, then $B_m = m$ for all $m \geq 1$.

Fibonacci: Take $P = (0, 0)$ on $C: y^2 + xy + y = x^3 - 2x^2$ and write $x(mP) = A_m/B_m^2$, then $(B_m)$ is the Fibonacci sequence.
In general if $C : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ has no singular points then we call $(B_m)$ an *elliptic divisibility sequence*. 
Questions: In a divisibility sequence...

1. are there finitely many terms without a primitive divisor (a prime divisor which does not divide any previous term)?
Questions: In a divisibility sequence...

1. are there finitely many terms without a primitive divisor (a prime divisor which does not divide any previous term)?

(Cornelissen and Zahidi: The existence of primitive divisors in suitable residue classes would resolve a certain quantifier elimination problem, first studied by Julia Robinson.)
Questions: In a divisibility sequence...

1. are there finitely many terms without a primitive divisor?
2. are there finitely many prime (power) terms?
Questions: In a divisibility sequence...

1. are there finitely many terms without a primitive divisor?

2. are there finitely many prime (power) terms?

(An elliptic divisibility sequence has a much larger growth rate than Mersenne.)
Questions: In a divisibility sequence...

1. are there finitely many terms without a primitive divisor?

2. are there finitely many prime (power) terms?

3. are there finitely many perfect power terms?
Questions: In a divisibility sequence...

1. are there finitely many terms without a primitive divisor?
2. are there finitely many prime (power) terms?
3. are there finitely many perfect power terms?

(This requires combining properties of the sequence with cutting edge modular techniques.)
The Arithmetic of Divisibility Sequences

We know the answers to all three questions for the integers...

1. There are infinitely many integers without a primitive divisor (e.g. $2^n$).
The Arithmetic of Divisibility Sequences

We know the answers to all three questions for the integers...

1. There are infinitely many integers without a primitive divisor (e.g. $2^n$).

2. There are infinitely many prime numbers (Euclid).
The Arithmetic of Divisibility Sequences

We know the answers to all three questions for the integers...

1. There are infinitely many integers without a primitive divisor (e.g. $2^n$).

2. There are infinitely many prime numbers (Euclid).

3. There are infinitely many perfect powers in $\mathbb{Z}$. 
Let $P = (-386, 4153)$ on $E: y^2 + xy = x^3 - 141875x + 18393057$.

Write $x(mP) = A_m / B_m^2$.
Example of an Elliptic Divisibility Sequence

Let \( P = (-386, 4153) \) on \( E : y^2 + xy = x^3 - 141875x + 18393057 \).

Write \( x(mp) = A_m/B_m^2 \).

\( B_m = 1 \) for \( m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 13, 14, 15, 16, 18 \) and 21.
Example of an Elliptic Divisibility Sequence

Let \( P = (-386, 4153) \) on \( E : y^2 + xy = x^3 - 141875x + 18393057 \).

Write \( x(mP) = A_m/B_m^2 \).

\( B_m = 1 \) for \( m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 13, 14, 15, 16, 18 \) and 21.

\( B_{28} = 5^2, \ B_{30} = 3^2, \ B_{34} = 2^3 \).
Example of an Elliptic Divisibility Sequence

Let $P = (-386, 4153)$ on $E : y^2 + xy = x^3 - 141875x + 18393057$. Write $x(mP) = A_m/B_m^2$.

$B_m = 1$ for $m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 13, 14, 15, 16, 18$ and 21. $B_{28} = 5^2, B_{30} = 3^2, B_{34} = 2^3$.

$B_m$ is prime for $m = 10, 11, 17, 19, 20, 22, 23, 24, 25, 26, 27, 29, 31, 32, 35, 36, 37, 39, 41, 42, 47, 49, 53, 61, 63, 67, 73, 83, 103, 163, 613$ and 1811 (32 terms).
Example of an Elliptic Divisibility Sequence

Let $P = (-386, 4153)$ on $E : y^2 + xy = x^3 - 141875x + 18393057$.

Write $x(mP) = A_m/B_m^2$.

$B_m = 1$ for $m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 13, 14, 15, 16, 18$ and $21$.

$B_{28} = 5^2$, $B_{30} = 3^2$, $B_{34} = 2^3$.

$B_m$ is prime for $m = 10, 11, 17, 19, 20, 22, 23, 24, 25, 26, 27, 29, 31, 32, 35, 36, 37, 39, 41, 42, 47, 49, 53, 61, 63, 67, 73, 83, 103, 163, 613$ and $1811$ (32 terms).

$B_{1811}$ has 6494 digits.
Let $P = (-386, 4153)$ on $E: y^2 + xy = x^3 - 141875x + 18393057$.

Write $x(mP) = A_m/B_m^2$.

$B_m = 1$ for $m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 13, 14, 15, 16, 18$ and $21$.

$B_{28} = 5^2$, $B_{30} = 3^2$, $B_{34} = 2^3$.

$B_m$ is prime for $m = 10, 11, 17, 19, 20, 22, 23, 24, 25, 26, 27, 29, 31, 32, 35, 36, 37, 39, 41, 42, 47, 49, 53, 61, 63, 67, 73, 83, 103, 163, 613$ and $1811$ (32 terms).

$B_{1811}$ has 6494 digits.

Note that $\hat{h}(P) = \lim_{n \to \infty} \log(B_{2n})/4^n = 0.009...$
1. (2001 Bilu, Hanrot, Voutier) All terms in a Lucas sequence beyond the 30th have a primitive divisor.
1. (2001 Bilu, Hanrot, Voutier) All terms in a Lucas sequence beyond the 30th have a primitive divisor.

(1988 Silverman) Finitely many terms in an elliptic divisibility sequence fail to have a primitive divisor.

(2010 Silverman and Ingram) If the Weierstrass equation is minimal and the abc conjecture holds then the number of terms without a primitive divisor is bounded independently of the sequence.
1. are there finitely many terms without a primitive divisor?

2. are there finitely many prime (power) terms?

The Fibonacci and Mersenne sequences are believed to have infinitely many prime terms.
1. are there finitely many terms without a primitive divisor?

2. are there finitely many prime (power) terms?

The Fibonacci and Mersenne sequences are believed to have infinitely many prime terms.

(Everest, Miller, Stephens, King, R.) If the polynomial

\[ \delta_n^P(x) = \prod_{R \in E(\bar{Q})} (x - x(R)) \in \mathbb{Q}[x] \]

such that \( nR = P \)

factorizes (over \( \mathbb{Q}[x] \)) for some \( n \) then the elliptic divisibility sequence generated by \( P \) has finitely many prime terms.
1. are there finitely many terms without a primitive divisor?

2. are there finitely many prime (power) terms?

3. are there finitely many perfect power terms?

(2001 Petho) There are finitely many perfect powers in a Lucas sequence.

(2006 Bugeaud, Mignotte, Siksek) The only perfect powers in the Fibonacci sequence are $1, 8 = 2^3$ and $144 = 12^2$. 

Jonathan Reynolds
Divisibility Sequences and Diophantine Equations
Perfect Powers in Elliptic Divisibility Sequences

Recall: $E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ $(a_i \in \mathbb{Z})$

$P \in E(\mathbb{Q})$ is a non-torsion point, $x(mP) = A_m/B_m^2$.
Recall: $E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ (a_i \in \mathbb{Z})$

$P \in E(\mathbb{Q})$ is a non-torsion point, $x(mP) = A_m/B_m^2$.

**Theorem (R.)** If 2 or 3 divides $B_1$ then there are finitely many perfect powers in $(B_m)$. 

**Theorem (Dahmen, R.)** If $j(E) = 1728$ (e.g. $E : y^2 = x^3 + a_4 x$) and $B_1 > 1$ then there are finitely many perfect powers in $(B_m)$. 

The proofs bound the exponent of the perfect power effectively!
Recall: $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ (a_i \in \mathbb{Z})$

$P \in E(\mathbb{Q})$ is a non-torsion point, $x(mP) = A_m/B_m^2$.

**Theorem (R.)** If 2 or 3 divides $B_1$ then there are finitely many perfect powers in $(B_m)$.

**Theorem (R.)** If $j(E) = 0$ (e.g. $E : y^2 = x^3 + a_6$) and $B_1 > 1$ then there are finitely many perfect powers in $(B_m)$.
Recall: $E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ ($a_i \in \mathbb{Z}$) $P \in E(\mathbb{Q})$ is a non-torsion point, $x(mP) = A_m/B_m^2$.

**Theorem** (R.) If 2 or 3 divides $B_1$ then there are finitely many perfect powers in $(B_m)$.

**Theorem** (R.) If $j(E) = 0$ (e.g. $E : y^2 = x^3 + a_6$) and $B_1 > 1$ then there are finitely many perfect powers in $(B_m)$.

**Theorem** (Dahmen, R.) If $j(E) = 1728$ (e.g. $E : y^2 = x^3 + a_4 x$) and $B_1 > 1$ then there are finitely many perfect powers in $(B_m)$.

The proofs bound the exponent of the perfect power effectively!
Substituting \((A_m/B_m^2, C_m/B_m^3)\) into \(y^2 = x^3 + D\) \((D = a_6 \in \mathbb{Z})\) with \(B_m = B^l\) gives

\[ C_m^2 - A_m^3 = DB^{6l}. \] (1)
Substituting \((A_m/B_m^2, C_m/B_m^3)\) into \(y^2 = x^3 + D\) \((D = a_6 \in \mathbb{Z})\) with \(B_m = B^l\) gives

\[ C_m^2 - A_m^3 = DB^{6l} \tag{1} \]

We know that for fixed \(l > 1\) there are finitely many solutions (Darmon and Granville).
Bounding $l$ in $C_m^2 - A_m^3 = DB^{6l}$, $B_m = B^l$

From modular methods (after Fermat’s Last Theorem) we get that if there exists a fixed prime $p$ such that $p | B_m$ and $p \nmid 6D$ then

$$l < (1 + \sqrt{p})^{2[K_f : \mathbb{Q}]},$$

where $[K_f : \mathbb{Q}]$ depends only on some fixed newform $f$ (a special type of modular form) and can be computed.
So if there exists a fixed prime $p$ such that $p \mid B_m$ and $p \nmid 6D$ then $l$ is bounded. Why should such a prime $p$ exist?
Bounding \( l \) in \( C_m^2 - A_m^3 = DB^{6l}, \ B_m = B^l \)

So if there exists a fixed prime \( p \) such that \( p \mid B_m \) and \( p \nmid 6D \) then \( l \) is bounded. Why should such a prime \( p \) exist?

Assume that \( B_1 > 1 \) and choose a prime \( q \mid B_1 \).
So if there exists a fixed prime $p$ such that $p \mid B_m$ and $p \nmid 6D$ then $l$ is bounded. Why should such a prime $p$ exist?

Assume that $B_1 > 1$ and choose a prime $q \mid B_1$.

Property of EDS: $\text{ord}_q(B_m) = \text{ord}_q(B_1) + \text{ord}_q(m)$. 

So if there exists a fixed prime $p$ such that $p \mid B_m$ and $p \nmid 6D$ then $l$ is bounded. Why should such a prime $p$ exist?

Assume that $B_1 > 1$ and choose a prime $q \mid B_1$.

Property of EDS: $\text{ord}_q(B_m) = \text{ord}_q(B_1) + \text{ord}_q(m)$.

Since $l \leq \text{ord}_q(B_m)$, $l - \text{ord}_q(B_1) \leq \text{ord}_q(m)$. 
Bounding \( l \) in \( C_m^2 - A_m^3 = DB^{6l}, \) \( B_m = B^l \)

So if there exists a fixed prime \( p \) such that \( p \mid B_m \) and \( p \nmid 6D \) then \( l \) is bounded. Why should such a prime \( p \) exist?

Assume that \( B_1 > 1 \) and choose a prime \( q \mid B_1 \).

Property of EDS: \( \text{ord}_q(B_m) = \text{ord}_q(B_1) + \text{ord}_q(m) \).

Since \( l \leq \text{ord}_q(B_m) \), \( l - \text{ord}_q(B_1) \leq \text{ord}_q(m) \).

We can fix \( e \) so that there exists \( p \mid B_q^e \) and \( p \nmid 6D \).
So if there exists a fixed prime $p$ such that $p \mid B_m$ and $p \nmid 6D$ then $l$ is bounded. Why should such a prime $p$ exist?

Assume that $B_1 > 1$ and choose a prime $q \mid B_1$.

Property of EDS: $\text{ord}_q(B_m) = \text{ord}_q(B_1) + \text{ord}_q(m)$.

Since $l \leq \text{ord}_q(B_m)$, $l - \text{ord}_q(B_1) \leq \text{ord}_q(m)$.

We can fix $e$ so that there exists $p \mid B_q^e$ and $p \nmid 6D$.

Then choosing $l > \text{ord}_q(B_1) + e$ gives $q^e \mid m$ so $p \mid B_q^e \mid B_m$. 
Theorem (R.) If \( j(E) = 0 \) (e.g. \( E : y^2 = x^3 + D \)) and \( B_1 > 1 \) then there are finitely many perfect powers in \((B_m)\).

Corollary. The only solutions to the Diophantine equation

\[
Y^2 = X^3 + 11Z^{6l}
\]

with \( l > 1 \) have \( Z = 0 \).

Corollary. The only solutions to the Diophantine equation

\[
U^3 + V^3 = 15W^{3l}
\]

with \( l > 1 \) have \( W = 0 \).
Recall: \( E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \) \((a_i \in \mathbb{Z})\)

\( P \in E(\mathbb{Q}) \) is a non-torsion point, \( x(mP) = A_m/B_m^2 \).

For \( j(E) = 1728 \) (e.g. \( E : y^2 = x^3 + Dx \)) and \( B_1 > 1 \) we use modularity of \( \mathbb{Q} \)-curves.
Recall: $E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ (a_i \in \mathbb{Z})$

$P \in E(\mathbb{Q})$ is a non-torsion point, $x(mP) = A_m/B_m^2$.

For $j(E) = 1728$ (e.g. $E : y^2 = x^3 + Dx$) and $B_1 > 1$ we use modularity of $\mathbb{Q}$-curves.

Again, the proof is effective: The only perfect power in the EDS generated by $P = (1/4, -9/8)$ on $E : y^2 = x^3 + 5x$ is $B_2 = 6^2$. 
What should be true for primes?

[Recall: If the polynomial

\[ \delta_n^P(x) = \prod_{R \in E(\overline{Q})} (x - x(R)) \in \mathbb{Q}[x] \]

such that \( nR = P \) factorizes (over \( \mathbb{Q}[x] \)) for some \( n \) then the elliptic divisibility sequence generated by \( P \) has finitely many prime terms.]

Conjecture. There exist EDS's for which \( \delta_n^P \) is irreducible for all \( n \).

R. This is true for all primes \( n \) and remains to be proven for all prime powers.

Are there infinitely many prime terms if \( \delta_n^P \) is irreducible for all \( n \)?
What should be true for primes?

[Recall: If the polynomial

\[ \delta_n^P(x) = \prod_{R \in E(\overline{Q})} (x - x(R)) \in \mathbb{Q}[x] \]

such that \( nR = P \)

factorizes (over \( \mathbb{Q}[x] \)) for some \( n \) then the elliptic divisibility sequence generated by \( P \) has finitely many prime terms.]

**Conjecture.** There exist EDS’s for which \( \delta_n \) is irreducible for all \( n \).

[R. This is true for all primes \( n \) and remains to be proven for all prime powers.]
What should be true for primes?

[Recall: If the polynomial

\[ \delta^n_P(x) = \prod_{R \in E(\overline{\mathbb{Q}})} (x - x(R)) \in \mathbb{Q}[x] \]

such that \( nR = P \)

factorizes (over \( \mathbb{Q}[x] \)) for some \( n \) then the elliptic divisibility sequence generated by \( P \) has finitely many prime terms.]

**Conjecture.** There exist EDS’s for which \( \delta_n \) is irreducible for all \( n \).

[R. This is true for all primes \( n \) and remains to be proven for all prime powers.]

Are there infinitely many prime terms if \( \delta_n \) is irreducible for all \( n \)?
What should be true for perfect powers?

Let \( x(P) = A/B^2 \) in lowest terms denote the \( x \)-coordinate of a rational point on an elliptic curve

\[
E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (a_i \in \mathbb{Z}).
\]
What should be true for perfect powers?

Let \( x(P) = A/B^2 \) in lowest terms denote the \( x \)-coordinate of a rational point on an elliptic curve

\[
E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (a_i \in \mathbb{Z}).
\]

If \( B \) is a perfect power then we could call such a point \textit{power integral} (since 1 is a perfect power).
What should be true for perfect powers?

Let $x(P) = A/B^2$ in lowest terms denote the $x$-coordinate of a rational point on an elliptic curve

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ (a_i \in \mathbb{Z}).$$

If $B$ is a perfect power then we could call such a point *power integral* (since 1 is a perfect power).

[Siegel. There are finitely many integral points in $E(\mathbb{Q})$ (points with $B = 1$).]
Let $x(P) = A/B^2$ in lowest terms denote the $x$-coordinate of a rational point on an elliptic curve

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ (a_i \in \mathbb{Z}).$$

If $B$ is a perfect power then we could call such a point *power integral* (since 1 is a perfect power).

[Siegel. There are finitely many integral points in $E(\mathbb{Q})$ (points with $B = 1$).]

[R. For fixed $l > 1$ there are finitely many points in $E(\mathbb{Q})$ with $B$ an $l$th power.]
Let $x(P) = A/B^2$ in lowest terms denote the $x$-coordinate of a rational point on an elliptic curve

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ (a_i \in \mathbb{Z}).$$

If $B$ is a perfect power then we could call such a point power integral (since 1 is a perfect power).

[Siegel. There are finitely many integral points in $E(\mathbb{Q})$ (points with $B = 1$).]

[R. For fixed $l > 1$ there are finitely many points in $E(\mathbb{Q})$ with $B$ an $l$th power.]

Fix a number field $K$. There are finitely many solutions to $u^4 + v^4 = w^l$ with $u, v, w \in \mathcal{O}_K$, $\gcd(u, v, w) = 1$ and $l > 2$ \Rightarrow There are finitely many power integral points in $E(\mathbb{Q})$. 
We know that for fixed $l > 1$ there are finitely many solutions.
We know that for fixed \( l > 1 \) there are finitely many solutions. Consider the Frey curve

\[
E : v^2 = u^3 - 3A_m u - 2C_m
\]

with \( \Delta_{\text{min}} = -2^{6l} 3^3 \text{DB}^6 \) and conductor

\[
N = 2^{\epsilon_2} 3^{\epsilon_3} \prod_{\text{primes } p | \text{DB}, \ p \neq 2,3} p,
\]

where \( \epsilon_2 \leq 7 \) and \( \epsilon_3 \leq 4 \) can be determined explicitly.
As is conventional, all newforms shall have weight 2 with a trivial character at some level $N$ and shall be thought of as a $q$-expansion

$$f = q + \sum_{n \geq 2} c_n q^n,$$

where the field $K_f = \mathbb{Q}(c_2, c_3, \ldots)$ is a totally real number field. The coefficients $c_n$ are algebraic integers.
As is conventional, all newforms shall have weight 2 with a trivial character at some level $N$ and shall be thought of as a $q$-expansion

$$f = q + \sum_{n \geq 2} c_n q^n,$$

where the field $K_f = \mathbb{Q}(c_2, c_3, \cdots)$ is a totally real number field. The coefficients $c_n$ are algebraic integers.
As is conventional, all newforms shall have weight 2 with a trivial character at some level $N$ and shall be thought of as a $q$-expansion

$$f = q + \sum_{n \geq 2} c_n q^n,$$

where the field $K_f = \mathbb{Q}(c_2, c_3, \cdots)$ is a totally real number field. The coefficients $c_n$ are algebraic integers.

- For a given level $N_0$, the number of newforms is finite.
Proposition (modularity + level-lowering; Wiles, Taylor, Ribet, Diamond, Conrad, Breuil):

Let \( E/\mathbb{Q} \) be an elliptic curve with conductor \( N \) and minimal discriminant \( \Delta_{\text{min}} \), \( l \) an odd prime and \( N_0(E, l) := N/\prod_{\text{primes } p \mid l} p^{ \text{ord}_p(\Delta_{\text{min}}) } \).

If the Galois representation \( \rho_E^l : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(E[l]) \) is irreducible then there exists a newform \( f \) of level \( N_0(E, l) \).
Proposition (modularity + level-lowering; Wiles, Taylor, Ribet, Diamond, Conrad, Breuil): Let \( E/\mathbb{Q} \) be an elliptic curve with conductor \( N \) and minimal discriminant \( \Delta_{\text{min}} \), \( l \) an odd prime and

\[
N_0(E, l) := N / \prod_{\text{primes } p \mid |N \text{ and } l \mid \text{ord}_p(\Delta_{\text{min}})} p.
\]
Proposition (modularity + level-lowering; Wiles, Taylor, Ribet, Diamond, Conrad, Breuil): Let $E/\mathbb{Q}$ be an elliptic curve with conductor $N$ and minimal discriminant $\Delta_{\text{min}}$, $l$ an odd prime and

$$N_0(E, l) := N / \prod_{\text{primes } p \mid |N \text{ and } l \mid \text{ord}_p(\Delta_{\text{min}})} p.$$ 

If the Galois representation

$$\rho_l^E : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}(E[l])$$

is irreducible then there exists a newform $f$ of level $N_0(E, l)$. 

Jonathan Reynolds  Divisibility Sequences and Diophantine Equations
We get that $N_0 \ (\leq 2^73^4D)$ is only divisible by primes dividing $6D$. 
We get that $N_0 (\leq 2^73^4 D)$ is only divisible by primes dividing $6D$.

For arbitrary $D$ there could be many newforms at level $N_0$. 
However: If $p$ is a prime such that $p \mid N$ and $p \nmid lN_0$. Then

There exists a prime $L$ lying above $l$ in the ring of integers $\mathcal{O}$ defined by the coefficients of $f$ such that $c_p \equiv (1 + p) \equiv 0 \pmod{L}$, where $c_p$ is the $p$th coefficient of $f$.

In particular, $l < (1 + \sqrt{p})^2$. 

However: If $p$ is a prime such that $p \mid N$ and $p \nmid lN_0$. Then

there exists a prime $\mathcal{L}$ lying above $l$ in the ring of integers $\mathcal{O}_f$
defined by the coefficients of $f$ such that

$$c_p \pm (1 + p) \equiv 0 \mod \mathcal{L},$$

where $c_p$ is the $p$th coefficient of $f$. 

In particular, $l < (1 + \sqrt{p})^2[K_f : \mathbb{Q}]$. 

Jonathan Reynolds
Divisibility Sequences and Diophantine Equations
However: If $p$ is a prime such that $p \mid |N$ and $p \nmid \mathcal{N}_0$. Then

- there exists a prime $\mathcal{L}$ lying above $l$ in the ring of integers $\mathcal{O}_f$ defined by the coefficients of $f$ such that

$$c_p \pm (1 + p) \equiv 0 \mod \mathcal{L},$$

where $c_p$ is the $p$th coefficient of $f$.

- In particular,

$$l < (1 + \sqrt{p})^{2[K_f:\mathbb{Q}]}.$$