Notes for A323748

Let $b \neq -1, 0, 1$ be an integer. A prime p is called a unique-period prime in base b if there is no other prime q such that $\mathrm{ord}_p(b) = \mathrm{ord}_q(b)$, where $\mathrm{ord}_m(a)$ is the multiplicative order of a modulo m. Let the Zsigmondy numbers $\mathrm{Zs}(n, a, b)$ ($n \in \mathbb{N}^*$; $a, b \in \mathbb{Z}$, $a, b \neq 0$, $|a| \neq |b|$) be defined as follows: $\mathrm{Zs}(n, a, b)$ is the largest divisor of $|a^n - b^n|$ that is coprime to $a^j - b^j$ for all $j < n$. (OEIS A323748 gives the values of $\mathrm{Zs}(n, k, 1)$ for $n \in \mathbb{N}^*$, $k \geq 2$.) An important observation is that p is a unique-period prime in base b if and only if $\mathrm{Zs}(\mathrm{ord}_p(b), b, 1) = p^e$ for some $e \geq 1$.

Given prime p, how to find bases b in which p is a unique-period prime? That amounts to finding the solutions (b, e) to $\mathrm{Zs}(n, b, 1) = p^e$, where $n|(p-1)$. Note that the cases $n = 1$ and $n = 2$ (when $p > 2$) are trivial: $\mathrm{Zs}(1, b, 1) = b - 1$, so $\mathrm{Zs}(n, b, 1) = p^e \Leftrightarrow b = p^e + 1 (e \geq 1)$; $\mathrm{Zs}(1, b, 1) = \mathrm{odd}(b+1)$ where odd means the odd part (OEIS A000265), so $\mathrm{Zs}(2, b, 1) = p^e \Leftrightarrow b = 2^{e_0} p^e - 1 (e_0 \geq 0, e \geq 1)$. We will assume that $n \geq 3$ later on. Here comes an important property of the Zsigmondy numbers: for $n \geq 3$, let $p_0 = \mathrm{gpf}(n)$ be the greatest prime factor of n, write $n = n_0 p_0^t$, $\gcd(n_0, p_0) = 1$. If $n_0|(p_0 - 1)$ (namely, n is in OEIS A342256), then $\mathrm{Zs}(n, b, 1)$ is either $\Phi_n(b)$ or $\Phi_n(b)/\mathrm{gpf}(n)$, where Φ_n is the n-th cyclotomic polynomial; otherwise (namely, $n = 12, 15, 24, 28, 30, 33, 35, \cdots$ is in OEIS A253235), then $\mathrm{Zs}(n, b, 1) = \Phi_n(b)$.

(a) If $n \geq 4$ is a power of 2, then $p \equiv 1 (\mathrm{mod}\ 4)$. We have $\mathrm{Zs}(n, b, 1) = b^{n/2} + 1$ or $(b^{n/2} + 1)/2$. So when is $\mathrm{Zs}(n, b, 1)$ equal to p^e? According to the parity of e we have four equations

$$(b^{n/4})^2 + 1 = (p^{e/2})^2, (b^{n/4})^2 + 1 = p(p^{(e-1)/2})^2, (b^{n/4})^2 + 1 = 2(p^{e/2})^2, (b^{n/4})^2 + 1 = 2p(p^{(e-1)/2})^2.$$

The first one is not possible; to solve the remaining three we need to find the solutions (x, y) to the Pell equations where y is a power of p

$$x^2 - py^2 = -1, x^2 - 2y^2 = -1, x^2 - 2py^2 = -1.$$

Let (x_0, y_0) be the fundamental solution to $x^2 - ry^2 = -1 (r \in \{2, p, 2p\})$, then by the theory of Pell equations, the solutions y are given by

$$y = \frac{(x_0 + y_0\sqrt{p})^m - (x_0 - y_0\sqrt{p})^m}{2\sqrt{p}},$$

where m is an odd number. Note that the sequence $\left\{ y_m = \dfrac{(x_0 + y_0\sqrt{p})^m - (x_0 - y_0\sqrt{p})^m}{2\sqrt{p}} \right\}_{m \in \mathbb{N}}$ is a Lucas sequence of the first kind, so it is a divisible sequence: $y_m | y_{m'}$ whenever $m|m'$. Suppose that m_0 is the smallest $m \in \mathbb{N}^*$ such that $p^e | y_m$, and that y_{m_0} is not a power of p, then $p^e | y_m$ would imply that y_m is also divisible by some non-power of p. In this case, the only possible case where y_m is a power of p is $y_m = 1, p, \cdots, p^{e-1}$.

Example. $p = 5$. The solutions y to $x^2 - 5y^2 = -1$ are

$$y = \frac{(2 + \sqrt{5})^m - (2 - 5\sqrt{5})^m}{2\sqrt{5}},$$

where m is an odd number. Let $y_m = \dfrac{(2 + \sqrt{5})^m - (2 - 5\sqrt{5})^m}{2\sqrt{5}}$, then $5^3 | y_m \Leftrightarrow 125 | m \Leftrightarrow y_{125} | y_m$. But y_{125} is not a power of 5, so y_m cannot be a power of 5 with exponent ≥ 3. The equations $x^2 - 2y^2 = -1$ and $x^2 - 10y^2 = -1$ can be similarly discussed.

(b) If n is odd but not squarefree, then we have the formula $\Phi_n(b) = \Phi_{\mathrm{rad}(n)}(b^{n/\mathrm{rad}(n)})$, where rad is the squarefree kernel (OEIS A007947). So the equation $\mathrm{Zs}(n, b, 1) = p^e$ can be written as either $\Phi_{\mathrm{rad}(n)}(b^{n/\mathrm{rad}(n)}) = p^e$ or $\Phi_{\mathrm{rad}(n)}(b^{n/\mathrm{rad}(n)}) = \mathrm{gpf}(n)p^e$ (if n is in A342256). Note that if n is in A342256, then so is $\mathrm{rad}(n)$.

(c) If n is even and not a power of 2, write $n = 2^r \cdot n'$ for odd n', then we have the formula $\Phi_n(b) = \Phi_{\mathrm{rad}(n')}(-b^{2^{r-1}n'/\mathrm{rad}(n')})$. So the equation $\mathrm{Zs}(n, b, 1) = p^e$ can be written as either $\Phi_{\mathrm{rad}(n')}(-b^{2^{r-1}n'/\mathrm{rad}(n')}) = p^e$ or $\Phi_{\mathrm{rad}(n')}(-b^{2^{r-1}n'/\mathrm{rad}(n')}) = \mathrm{gpf}(n)p^e$ (if n is in A342256). Note that if n is in A342256, then so is $\mathrm{rad}(n')$.

The cases (b) and (c) can both be reduced to the case where n is an odd squarefree number ≥ 3, and the equations in question are $\Phi_n(b) = p^e$ and $\Phi_n(b) = \mathrm{gpf}(n)p^e$ (if n is in A342256). The following is a list of the values of n and the equations that needs to be considered.

p	Values of n	Equations to study
2	–	–
3	–	–
5	–	–
7	3	$x^2+x+1=7^e, x^2+x+1=3\cdot 7^e$
11	5	$x^4+x^3+x^2+x+1=11^e, x^4+x^3+x^2+x+1=3\cdot 11^e$
13	3	$x^2+x+1=13^e, x^2+x+1=3\cdot 13^e$
17	–	–
19	3	$x^2+x+1=19^e, x^2+x+1=3\cdot 19^e$
23	11	$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1=23^e$, $x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1=11\cdot 23^e$
29	7	$x^6+x^5+x^4+x^3+x^2+x+1=29^e$, $x^6+x^5+x^4+x^3+x^2+x+1=7\cdot 29^e$
31	3	$x^2+x+1=31^e, x^2+x+1=3\cdot 31^e$
	5	$x^4+x^3+x^2+x+1=31^e, x^4+x^3+x^2+x+1=5\cdot 31^e$
	15	$x^8-x^7+x^5-x^4+x^3-x+1=31^e$
37	3	$x^2+x+1=37^e, x^2+x+1=3\cdot 37^e$

Remark. To find the solutions to $x^2+x+1=p^e$ and $x^2+x+1=3p^e$ for $p \equiv 1 \pmod 3$, one can imitate the method mentioned here.

Now we write these equations as Diophantine equations, where $n \geq 3$ is an odd squarefree factor of $p-1$. First suppose that $n > 3$. If n is in A342256, according to the parity of e we have four equations

$$\Phi_n(b) = (p^{e/2})^2, \Phi_n(b) = p(p^{(e-1)/2})^2, \Phi_n(b) = \mathrm{gpf}(n)(p^{e/2})^2, \Phi_n(b) = \mathrm{gpf}(n)p(p^{(e-1)/2})^2;$$

if n is in A253235, only the first two are present. So we need to find the solutions (b, y) where y is a power of p to

$$\Phi_n(b) = y^2, \Phi_n(b) = py^2, \Phi_n(b) = \mathrm{gpf}(n)y^2, \Phi_n(b) = \mathrm{gpf}(n)py^2$$

(if n is in A253235, only the first two are present). Note that Φ_n has degree ≥ 4, by Faltings's theorem, each equation has only finitely many integer solutions.

If $n = 3$, according to the remainder of e modulo 3 we have six equations

$$x^2 + x + 1 = (p^{e/3})^3, x^2 + x + 1 = p(p^{(e-1)/2})^3, x^2 + x + 1 = p^2(p^{(e-2)/2})^3,$$
$$x^2 + x + 1 = 3(p^{e/3})^3, x^2 + x + 1 = 3p(p^{(e-1)/2})^3, x^2 + x + 1 = 3p^2(p^{(e-2)/2})^3,$$

So we need to find the solutions (b, y) where y is a power of p to

$$x^2 + x + 1 = y^3, x^2 + x + 1 = py^3, x^2 + x + 1 = p^2y^3, x^2 + x + 1 = 3y^3, x^2 + x + 1 = 3py^3, x^2 + x + 1 = 3p^2y^3.$$

Each equation also has only finitely many integer solutions.

In conclusion, since there are only finitely many equations and each equation has only finitely many integer solutions, we know that the "exceptional" bases b subject to $n \geq 3$ are only finitely many.

The following is a list of what Diophantine equations to study for different p. Keep in mind the solutions y we need are the powers of p. Note that $x^4 + x^3 + x^2 + x + 1 = y^2$ $(n = 5)$ are easily seen to only have solutions $(0, \pm 1), (3, \pm 11)$ (see here for an example of a proof), so this equation is not listed.

p	Values of n	Diophantine equations to study
2	–	–
3	–	–
5	–	–
7	3	$x^2 + x + 1 = y^3, x^2 + x + 1 = 7y^3, x^2 + x + 1 = 49y^3,$ $x^2 + x + 1 = 3y^3, x^2 + x + 1 = 21y^3, x^2 + x + 1 = 147y^3$
11	5	$x^4 + x^3 + x^2 + x + 1 = 11y^2, x^4 + x^3 + x^2 + x + 1 = 5y^2, x^4 + x^3 + x^2 + x + 1 = 55y^2$
13	3	$x^2 + x + 1 = y^3, x^2 + x + 1 = 13y^3, x^2 + x + 1 = 169y^3,$ $x^2 + x + 1 = 3y^3, x^2 + x + 1 = 39y^3, x^2 + x + 1 = 507y^3$
17	–	–
19	3	$x^2 + x + 1 = y^3, x^2 + x + 1 = 19y^3, x^2 + x + 1 = 361y^3,$ $x^2 + x + 1 = 3y^3, x^2 + x + 1 = 57y^3, x^2 + x + 1 = 1083y^3$
23	11	$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = y^2,$ $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 23y^2,$ $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 11y^2,$ $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 253y^2$
29	7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = y^2,$ $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 29y^2,$ $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 7y^2,$ $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 203y^2$
31	3	$x^2 + x + 1 = y^3, x^2 + x + 1 = 31y^3, x^2 + x + 1 = 961y^3,$ $x^2 + x + 1 = 3y^3, x^2 + x + 1 = 93y^3, x^2 + x + 1 = 2883y^3$
	5	$x^4 + x^3 + x^2 + x + 1 = 31y^2, x^4 + x^3 + x^2 + x + 1 = 5y^2, x^4 + x^3 + x^2 + x + 1 = 155y^2$
	15	$x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 = y^2, x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 = 31y^2$
37	3	$x^2 + x + 1 = y^3, x^2 + x + 1 = 37y^3, x^2 + x + 1 = 1369y^3,$ $x^2 + x + 1 = 3y^3, x^2 + x + 1 = 111y^3, x^2 + x + 1 = 4107y^3$

Remark. For $p = 11$: The equations $x^4 + x^3 + x^2 + x + 1 = 11y^2, x^4 + x^3 + x^2 + x + 1 = 5y^2, x^4 + x^3 + x^2 + x + 1 = 55y^2$ can be transformed into elliptic curve equations.

(1) Write

$$X = 33 \cdot \frac{19x^2 + 7x + 66y + 4}{x^2 + 4x + 4}, Y = \pm 3267 \cdot \frac{7x^3 + 4x^2 + 23xy + x + 2y - 2}{x^3 + 6x^2 + 12x + 8},$$

The equation $11y^2 = x^4 + x^3 + x^2 + x + 1$ becomes

$$Y^2 = X^3 - 32670X - 898425.$$

(2) Write

$$X = 75 \cdot \frac{2x^2 + 2x + 6y + 2}{x^2 - 2x + 1}, Y = \pm 3375 \cdot \frac{x^3 + x^2 + 2xy + x + 2y + 1}{x^3 - 3x^2 + 3x - 1},$$

The equation $5y^2 = x^4 + x^3 + x^2 + x + 1$ becomes

$$Y^2 = X^3 - 6750X - 84375.$$

(3) Write

$$X = 825 \cdot \frac{8x^2 + 3x + 66y + 3}{4x^2 + 12x + 9}, Y = \pm 408375 \cdot \frac{2x^3 + x^2 + 14xy - y - 1}{8x^3 + 36x^2 + 54x + 27},$$

The equation $55y^2 = x^4 + x^3 + x^2 + x + 1$ becomes

$$Y^2 = X^3 - 816750X - 112303125.$$