合同式

志甫　淳

東京大学大学院数理科学研究科

2021 年 11 月 21–23 日
2021 年度公開講座「p 進数」

合同式とは？

日常生活や算数，数学の授業などで次のようなことを考えたことがあると思います．

- 金曜日の 3 日前は火曜日，金曜日の 3 日後は月曜日である．
- 偶数＋偶数は偶数，偶数＋奇数は奇数になり，奇数＋奇数は偶数になる．
- 1 の位が 6 である数を何乗しても，その 1 の位は 6 のままである．

これらは合同式の計算例です．

この講演の目的は，合同式の計算をいろいろと行ってみることです．

合同式とは？

合同式の定義をしましょう．

定義

n を自然数 (1 以上の整数) とする．
整数 a, b に対して，その差 $a - b$ が n で割り切れるとき
a と b は n を法として合同であるといい，

$$a \equiv b \pmod{n}$$

と書く．このような式を合同式という．

例えば，
偶数とは 2 を法として 0 と合同な整数，
奇数とは 2 を法として 1 と合同な整数のことです．

あるいは，

$$12 \equiv 19 \pmod{7}, \qquad 37 \equiv 4 \pmod{11}$$

となります．

合同式とは？

整数 a を n で割ったときの商を q, 余りを r と書くと
$a = nq + r$，つまり $a - r = nq$ なので $a \equiv r \pmod{n}$ となります．

余り r は 0 以上 $n-1$ 以下の整数なので，整数 a は，$0, 1, \ldots, n-1$ の
いずれかと n を法として合同であるということがわかります．

つまり，n を法として合同である整数たちを同一視して考えた場合，
「数」は $0, 1, \ldots, n-1$ の n 個しかないということになります．

曜日の例で言うと，曜日が
日曜日，月曜日，火曜日，水曜日，木曜日，金曜日，土曜日
の７つしかないことと対応します．

合同式の性質

合同式の基本的な性質を述べます．

命題１

n を自然数とし，a, b, c, d を整数とする．
もし $a \equiv b \pmod{n}$，$c \equiv d \pmod{n}$ ならば

$$a + c \equiv b + d \pmod{n}, \quad a - c \equiv b - d \pmod{n}, \quad ac \equiv bd \pmod{n}$$

が成り立つ．

例えば，a, b が奇数のとき $a \equiv 1 \pmod{2}$，$b \equiv 1 \pmod{2}$ なので，
命題１より

$$a + b \equiv 1 + 1 \equiv 2 \equiv 0 \pmod{2}$$

となり，従って $a + b$ は偶数となります．つまり，奇数＋奇数は偶数になるということです．あるいは，

$$ab \equiv 1 \cdot 1 \equiv 1 \pmod{2}$$

なので ab は奇数となります．つまり，奇数×奇数は奇数になるということです．

合同式の性質

命題１の証明.

仮定 $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$ より，ある整数 k, l を用いて
$a - b = kn,\ c - d = ln$ と書ける．すると

$$(a + c) - (b + d) = (a - b) + (c - d) = kn + ln = (k + l)n,$$
$$(a - c) - (b - d) = (a - b) - (c - d) = kn - ln = (k - l)n,$$
$$ac - bd = (a - b)c + b(c - d) = knc + bln = (kc + bl)n$$

なので，

$$a + c \equiv b + d \pmod{n}, \quad a - c \equiv b - d \pmod{n}, \quad ac \equiv bd \pmod{n}$$

となる．

曜日の例

曜日の例に戻ってみましょう．

年月日による日付の表示 (例えば 2021 年 11 月 19 日) と曜日を結びつけるのは難しいので，1900 年 1 月 1 日 月曜日を 1 日目として数えた日数で日付を表すことにします．
(例えば，1900 年 1 月 2 日は 2, 2021 年 11 月 19 日は 44518 となります.)

このとき，日付を 7 で割った余りが
1 ならば月曜日，2 ならば火曜日，3 ならば水曜日，4 ならば木曜日，
5 ならば金曜日，6 ならば土曜日，0 ならば日曜日
ということになります．

言い換えると，日付 d の曜日は $d \equiv i \pmod 7$ となる $0 \leq i \leq 6$ に対応する曜日である，ということになります．
例えば，$44518 \equiv 5 \pmod 7$ なので 2021 年 11 月 19 日は金曜日です．

曜日の例

すると，金曜日である日 d の 3 日前の日 $d-3$ の曜日は
$d-3 \equiv 5-3 \equiv 2 \pmod 7$ より火曜日となります．

また，金曜日である日 d の 3 日後の日 $d+3$ の曜日は
$d+3 \equiv 5+3 \equiv 8 \equiv 1 \pmod 7$ より月曜日となります．

では，金曜日の 44 日後は何曜日でしょうか？

$5+44 \equiv 49 \equiv 0 \pmod 7$ より日曜日になります．

余談：日付と曜日との関係

これは余談ですが，年月日による日付の表示と曜日との関係として，次のツェラーの公式が知られています：西暦 y 年 m 月 d 日の曜日は

$$i \equiv y + [\tfrac{y}{4}] - [\tfrac{y}{100}] + [\tfrac{y}{400}] + [\tfrac{13m+8}{5}] + d \pmod 7$$

を満たす $0 \leq i \leq 6$ に対応する曜日である．
但し，$[x]$ は x を超えない最大の整数を表す．
また，$m = 1, 2$ のときは西暦 $(y-1)$ 年 $(m+12)$ 月 d 日とみて計算する．

例えば，2021 年 11 月 19 日の場合，

$$\begin{aligned} &2021 + [\tfrac{2021}{4}] - [\tfrac{2021}{100}] + [\tfrac{2021}{400}] + [\tfrac{13\cdot 11+8}{5}] + 19 \\ &\equiv 2021 + 505 - 20 + 5 + 30 + 19 \\ &\equiv 2560 \equiv 5 \pmod 7 \end{aligned}$$

より，金曜日であることがわかります．

1 の位の数

最初に挙げた次の問題を考えてみましょう．

- 1 の位が 6 である数を何乗しても，その 1 の位は 6 のままである．

1 の位を考えるというのは，自然数を 10 で割った余りを考える，つまり，10 を法として考えるということなので，この問題を合同式を用いて書くと次のようになります．

- $d \equiv 6 \pmod{10}$ である自然数 d と整数 $n \geq 1$ に対して $d^n \equiv 6 \pmod{10}$ である．

これは n に関する数学的帰納法により証明出来ます：実際，$n = 1$ のときは $d^1 \equiv d \equiv 6 \pmod{10}$ であり，また，$d^n \equiv 6 \pmod{10}$ であるとき $d^{n+1} \equiv d^n \cdot d \equiv 6 \cdot 6 \equiv 36 \equiv 6 \pmod{10}$ となります．これで上の問題も合同式の性質を使って解けました．

1 の位の数

では，3^{63} の 1 の位の数はいくつでしょうか？

$3^1 \equiv 3 \pmod{10}$, $\quad 3^2 \equiv 3 \cdot 3 \equiv 9 \pmod{10}$,
$3^3 \equiv 9 \cdot 3 \equiv 27 \equiv 7 \pmod{10}$, $\quad 3^4 \equiv 7 \cdot 3 \equiv 21 \equiv 1 \pmod{10}$
となります．従って

$$3^{63} \equiv (3^4)^{15} 3^3 \equiv 1^{15} \cdot 7 \equiv 7 \pmod{10}$$

となります．つまり，3^{63} の 1 の位の数は 7 であることがわかりました．

下 2 桁の数

更に考えます．3^{63} の下 2 桁の数はいくつでしょうか？

下 2 桁の数を考えるというのは，自然数を 100 で割った余りを考える，
つまり，100 を法として考えるということになります．

$3^1 \equiv 3 \pmod{100}$, $\quad 3^2 \equiv 3 \cdot 3 \equiv 9 \pmod{100}$,
$3^3 \equiv 9 \cdot 3 \equiv 27 \pmod{100}$, $\quad 3^4 \equiv 27 \cdot 3 \equiv 81 \pmod{100}$
$3^5 \equiv 81 \cdot 3 \equiv 243 \equiv 43 \pmod{100}$, $\ldots$

3^6 以降は，100 を法として順に
$29, 87, 61, 83, 49, 47, 41, 23, 69, 7, 21, 63, 89, 67, 1$
と合同になり，よって $3^{20} \equiv 1 \pmod{100}$ となります．従って

$$3^{63} \equiv (3^{20})^3 3^3 \equiv 1^3 \cdot 27 \equiv 27 \pmod{100}$$

となります．つまり，3^{63} の下 2 桁の数は 27 であることがわかりました．

下 2 桁の数

3^{63} の下 2 桁の数について，次のように工夫して求めることもできます．

まず，$3^2 \equiv 9 \equiv -1 + 10 \pmod{100}$ です．

すると，$3^{20} \equiv (-1+10)^{10} \equiv \sum_{i=0}^{10} {}_{10}\mathrm{C}_i (-1)^{10-i} 10^i \pmod{100}$
となります．

ここで，右辺の $i = 1$ のときの項 ${}_{10}\mathrm{C}_1 (-1)^9 10^1 = -10^2$ は 10^2 で
割り切れ，また，$2 \leq i \leq 10$ のときの項 ${}_{10}\mathrm{C}_i (-1)^{10-i} 10^i$ も 10^2 で割り切れます．よって $i = 0$ の項のみが残り，
$3^{20} \equiv \sum_{i=0}^{10} {}_{10}\mathrm{C}_i (-1)^{10-i} 10^i \equiv 1 \pmod{100}$ となります．

従って，$3^{63} \equiv (3^{20})^3 3^3 \equiv 1^3 \cdot 27 \equiv 27 \pmod{100}$ となります．

合同式の性質

合同式の性質をもう 1 つ紹介します．

命題 2

n を自然数とし，$n = p_1^{e_1} \cdots p_r^{e_r}$ をその素因数分解とする．このとき

$$a \equiv b \pmod{n} \iff \text{全ての } 1 \leq i \leq r \text{ に対して } a \equiv b \pmod{p_i^{e_i}}.$$

例えば $17 \equiv 5 \pmod{2^2}$, $17 \equiv 5 \pmod{3}$ なので $17 \equiv 5 \pmod{12}$.

命題 2 の証明

$$\begin{aligned}
& a \equiv b \pmod{n} \\
\iff & a - b \text{ が } n \text{ で割り切れる} \\
\iff & \text{全ての } 1 \leq i \leq r \text{ に対して } a - b \text{ が } p_i^{e_i} \text{ で割り切れる} \\
\iff & \text{全ての } 1 \leq i \leq r \text{ に対して } a \equiv b \pmod{p_i^{e_i}}.
\end{aligned}$$

命題 2 より，合同式の計算においては，素数のべき p^e を法とした合同式を考えることが本質的である，ということがわかります．

$\mathrm{mod}\, p$ での 1 次方程式

以下，合同式の世界で方程式を解くことを考えたいと思います．

合同式の計算においては，素数のべき p^e を法とした合同式を考えることが本質的でしたので，その場合に限定して考えます．

まずは素数 p を法とした合同式の世界で方程式を考えます．

変数 x に関する 1 次方程式 $ax \equiv b \pmod{p}$ は解けるでしょうか？
但し，$a \not\equiv 0 \pmod{p}$ であるとします．

$\mathrm{mod}\, p$ の合同式の性質

素数 p を法とする合同式の性質を 1 つ示します．

命題 3

p を素数とするとき，
$ab \equiv 0 \pmod{p} \iff a \equiv 0 \pmod{p}$ または $b \equiv 0 \pmod{p}$

命題 3 の証明

$$
\begin{aligned}
& ab \equiv 0 \pmod{p} \\
\iff\ & ab \text{ が } p \text{ で割り切れる } (p \text{ を素因子に持つ}) \\
\iff\ & a \text{ が } p \text{ で割り切れるまたは } b \text{ が } p \text{ で割り切れる} \\
\iff\ & a \equiv 0 \pmod{p} \text{ または } b \equiv 0 \pmod{p}
\end{aligned}
$$

$\mathrm{mod}\, p$ での 1 次方程式

変数 x に関する 1 次方程式 $ax \equiv b \pmod{p}$ (但し $a \not\equiv 0 \pmod{p}$)
の話に戻ります．

p 個の整数 $a \cdot 0,\ a \cdot 1,\ \ldots,\ a \cdot (p-1)$ を考えます．
$0 \leq i, j \leq p-1$ に対して，$ai \equiv aj \pmod{p}$ が成り立つとすると
$a(i-j) \equiv 0 \pmod{p}$ で，いま $a \not\equiv 0 \pmod{p}$ なので，命題３より
$i - j \equiv 0 \pmod{p}$ となります．$-(p-1) \leq i-j \leq p-1$ なので，
この合同式より $i = j$ を得ます．

従って，上の p 個の整数を p を法として考えても，それらが全て異なる
ことがわかります．p を法として合同なものを同一視した場合，
「数」は p 個しかありませんから，その全てが現れていることになり，
よって，ある i に対して $ai \equiv b \pmod{p}$ となることがわかります．つまり，
上の 1 次方程式は解け，また，p を法として合同なものを同一視した場合，
解は 1 つです．

$\mathrm{mod}\, p$ での 2 次方程式

変数 x に関する 2 次方程式 $ax^2 + bx + c \equiv 0 \pmod{p}$ は
解けるでしょうか？但し，$a \not\equiv 0 \pmod{p}$ であるとします．

まず，1 次方程式を解くことにより $ab' \equiv b \pmod{p},\ ac' \equiv c \pmod{p}$
を満たす b', c' があることがわかります．このとき

$$ax^2 + bx + c \equiv a(x^2 + b'x + c') \pmod{p}$$

で，また，仮定より $a \not\equiv 0 \pmod{p}$ なので，もとの方程式

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

は

$$x^2 + b'x + c' \equiv 0 \pmod{p}$$

と同値であることがわかります．従って，最初の方程式で $a = 1$ の場合だ
けを考えれば充分です．以下，

$$x^2 + bx + c \equiv 0 \pmod{p}$$

について考えましょう．

$\mathrm{mod}\, p$ での 2 次方程式

通常の 2 次方程式の場合と同様に，平方完成することを考えましょう．
以下しばらくは，$p \neq 2$，すなわち $2 \not\equiv 0 \pmod{p}$ であると仮定します．
すると，$2b' \equiv b \pmod{p}$ を満たす b' があり，このとき，方程式

$$x^2 + bx + c \equiv 0 \pmod{p}$$

は，

$$(x + b')^2 \equiv b'^2 - c \pmod{p}$$

と書き直すことができます．従って，2 次方程式は

$$x^2 \equiv c \pmod{p}$$

の形のものを考えれば十分であることがわかります．

これは解けるでしょうか？

$\mathrm{mod}\, p$ での 2 次方程式

p 個の整数 $0^2,\ 1^2,\ \ldots,\ (p-1)^2$ を考えます．

$0 \leq i, j \leq p-1$ に対して，$i^2 \equiv j^2 \pmod{p}$ が成り立つとすると
$i^2 - j^2 \equiv 0 \pmod{p}$，よって $(i-j)(i+j) \equiv 0 \pmod{p}$ であり，従って
$i - j \equiv 0 \pmod{p}$ または $i + j \equiv 0 \pmod{p}$ となります．
$-(p-1) \leq i - j \leq p-1,\ 0 \leq i + j \leq 2(p-1)$ なので，
この合同式より $i = j$ または $i + j = 0$ または $i + j = p$ となりますが，
$i + j = 0$ のときは $i = j = 0$ なので，結局 $i = j$ または $i + j = p$
となります．

従って，p を法として考えたとき，上の p 個の整数のうち
$0^2 = 0$ 以外のものについては

$$1^2 \equiv (p-1)^2 \pmod{p},\ 2^2 \equiv (p-2)^2 \pmod{p},\ \cdots$$

と 2 つずつが同じ「数」を表しており，得られる「数」の個数は
$1 + \frac{p-1}{2} = \frac{p+1}{2}$ 個となります．

$\mathrm{mod}\, p$ での 2 次方程式

従って，2 次方程式 $x^2 \equiv c \pmod{p}$ の解について，次のことが言えます．

$c \equiv 0 \pmod{p}$ のときはこの方程式はただ１つの解 $x \equiv 0 \pmod{p}$ (重解) を持ちます．

それ以外の c (を p を法として考えたもの) のうち $\frac{p-1}{2}$ 個については，この方程式は 2 つの解を持ちます．残りの $\frac{p-1}{2}$ 個については，この方程式は解を持ちません．

例えば，$p = 5$ のとき

$$0^2 \equiv 0 \pmod{5},\ 1^2 \equiv 4^2 \equiv 1 \pmod{5},\ 2^2 \equiv 3^2 \equiv 4 \pmod{5}$$

なので，2 次方程式 $x^2 \equiv c \pmod{p}$ は，$c = 0$ のとき重解を持ち，$c = 1, 4$ のとき 2 つの解を持ち，$c = 2, 3$ のときは解を持ちません．

$\mathrm{mod}\, p$ での 2 次方程式

$p = 2$ のときは，平方完成ができるとは限らないので，方程式

$$x^2 + bx + c \equiv 0 \pmod 2$$

を考えます．$x \equiv 0, 1 \pmod 2$ が解になるかどうかを代入して確かめることにより，次を得ます．

$x^2 \equiv 0 \pmod 2$ は重解 $x \equiv 0 \pmod 2$ を持ちます．

$x^2 + 1 \equiv 0 \pmod 2$ は重解 $x \equiv 1 \pmod 2$ を持ちます．

$x^2 + x \equiv 0 \pmod 2$ は 2 つの解 $x \equiv 0, 1 \pmod 2$ を持ちます．

$x^2 + x + 1 \equiv 0 \pmod 2$ は解を持ちません．

$\mathrm{mod}\, p^2$ での 1 次方程式

次に，p^2 を法とした合同式の世界で方程式を考えます．

変数 x に関する 1 次方程式 $ax \equiv b \pmod{p^2}$ は解けるでしょうか？

一般に，合同式について $s \equiv t \pmod{p^2}$ が成り立てば，$s \equiv t \pmod{p}$ が成り立ちます (両辺の差が p^2 で割り切れるならば，p で割り切れる) ので，このことを利用して p を法とした合同式と関連付けて考えることにします．

$a \not\equiv 0 \pmod{p^2}$ と仮定しても，1 次方程式 $ax \equiv b \pmod{p^2}$ は解けないことがあります．例えば，$a = p, b = 1$ としたときの方程式 $px \equiv 1 \pmod{p^2}$ が解を持ったとすると，$px \equiv 1 \pmod{p}$ も解を持つことになりますが，これは $0 \equiv 1 \pmod{p}$ という式になっていますので，決して成り立ちません．

しかしながら，$a \not\equiv 0 \pmod{p}$ と仮定すれば，上の 1 次方程式は
解を持つことが言えます．それを確かめてみましょう．

$\bmod p^2$ での 1 次方程式

$ax \equiv b \pmod{p^2}$ が成り立てば，$ax \equiv b \pmod{p}$ が成り立つので，
前者の解は後者の解となります．

この逆は成り立ちませんが，$ax \equiv b \pmod{p}$ の (p を法として考えた場合にただ 1 つである) 解 x_0 をとり，それを適切に修正することによって，
$x \equiv x_0 \pmod{p}$ であるような $ax \equiv b \pmod{p^2}$ の解を構成することを考えます．

$ax_0 \equiv b \pmod{p}$ なので，$b - ax_0 = pd$ と書けます．また，解の候補を $x = x_0 + px_1$ と置きます．すると

$$\begin{aligned} ax \equiv b \pmod{p^2} &\iff a(x_0 + px_1) \equiv b \pmod{p^2} \\ &\iff p(ax_1 - d) \equiv 0 \pmod{p^2} \end{aligned}$$

です．最後の式は $p(ax_1 - d)$ が p^2 で割り切れることを表しており，それは $ax_1 - d$ が p で割り切れることと同値なので $ax_1 \equiv d \pmod{p}$ と同値です．
$a \not\equiv 0 \pmod{p}$ なので，これはただ 1 つの解 x_1 を持ちます．

従って，1 次方程式 $ax \equiv b \pmod{p^2}$ は，$a \not\equiv 0 \pmod{p}$ のとき，
(p^2 を法として考えた場合に) ただ 1 つの解を持ちます．

$\mathrm{mod}\, p^2$ での 2 次方程式

次に，2 次方程式 $ax^2 + bx + c \equiv 0 \pmod{p^2}$ を
考えましょう．但し，$a \not\equiv 0 \pmod{p}$ であるとします．

p を法として考えた場合と同様の議論により，$x^2 + bx + c \equiv 0 \pmod{p^2}$ の
形の 2 次方程式を考えれば充分であることがわかります．

以下，しばらくは $p \neq 2$ であると仮定します．
すると，p を法として考えた場合と同様に平方完成ができて，
$x^2 \equiv c \pmod{p^2}$ の形の 2 次方程式を考えれば充分であることが
わかります．

さきほどと同じように，2 次方程式 $x^2 \equiv c \pmod{p}$ と関連付けて
考えましょう．

$\mathrm{mod}\, p^2$ での 2 次方程式

(1) $c \equiv 0 \pmod{p}$ のとき

2 次方程式 $x^2 \equiv c \pmod{p}$ の解は 0 のみ (重解) なので，$x^2 \equiv c \pmod{p^2}$ 解の候補は px_1 と書けます．すると

$$x^2 \equiv c \pmod{p^2} \iff p^2x_1^2 \equiv c \pmod{p^2} \iff 0 \equiv c \pmod{p^2} \cdots\cdots (*)$$

です．さらに場合分けをします．

(1-1) $c \equiv 0 \pmod{p^2}$ のとき

このときは，(*) はどのような x_1 に対しても成り立ち，解 $x = px_1$ は $0, p, \ldots, (p-1)p$ の p 個になります．

なお，2 次方程式なのに (2 個より多い) p 個解を持つことになっていますが，これは $p^e\ (e \geq 2)$ を法とする合同式で考えた場合には起こりえることです．

(1-2) $c \not\equiv 0 \pmod{p^2}$ のとき

(つまり $c \equiv p, 2p, \cdots, (p-1)p \pmod{p^2}$ のとき)

このときは，(*) は決して成り立たないので，解はありません．

$\mathrm{mod}\, p^2$ での 2 次方程式

(2) $c \not\equiv 0 \pmod{p}$ のとき　さらに場合分けをします．

(2-1) $x^2 \equiv c \pmod{p}$ が解を持たないとき

このときは，$x^2 \equiv c \pmod{p^2}$ も解を持つことはありません．

(2-2) $x^2 \equiv c \pmod{p}$ が解を持つとき

2 次方程式 $x^2 \equiv c \pmod{p}$ は 2 つ解を持ちます．それを x_0, x_0' とすると，解の候補は $x = x_0 + px_1, x_0' + px_1'$ と書けます．また，$c - x_0^2 = pd$, $c - {x_0'}^2 = pd'$ と書けます．すると，$x = x_0 + px_1$ の方を考えた場合，

$$
\begin{aligned}
& x^2 \equiv c \pmod{p^2} \Longrightarrow (x_0 + px_1)^2 \equiv c \pmod{p^2} \\
\iff\ & x_0^2 + 2px_1 \equiv c \pmod{p^2} \iff 2px_1 \equiv pd \pmod{p^2} \\
\iff\ & 2x_1 \equiv d \pmod{p}
\end{aligned}
$$

となります．これはただ 1 つの解 x_1 を持ちます．$x = x_0' + px_1'$ の方を考えた場合も同様にただ 1 つの解 x_1' を持ちます．結局，この場合は方程式 $x^2 \equiv c \pmod{p^2}$ は (p^2 を法として考えて)2 つ解を持ちます．

p を法として考えた方程式 $x^2 \equiv c \pmod{p}$ が 2 つ解を持つときは，2 つの解それぞれが $x^2 \equiv c \pmod{p^2}$ の解に一意的に持ち上がっていることがわかります．

$\bmod p^2$ での 2 次方程式

$p = 2$ のときに 2 次方程式

$$x^2 + bx + c \equiv 0 \pmod{2^2}$$

を考えます．結果だけ書いておきましょう．

$x^2 \equiv 0 \pmod{2^2}$ は 2 つの解 $x \equiv 0, 2 \pmod{2^2}$ を持ちます．

$x^2 \equiv 1 \pmod{2^2}$ は 2 つの解 $x \equiv 1, 3 \pmod{2^2}$ を持ちます．

$x^2 \equiv 2 \pmod{2^2}$, $x^2 \equiv 3 \pmod{2^2}$ は解を持ちません．

$x^2 + x \equiv 0 \pmod{2^2}$ は 2 つの解 $x \equiv 0, 3 \pmod{2^2}$ を持ちます．

$x^2 + 3x \equiv 0 \pmod{2^2}$ は 2 つの解 $x \equiv 0, 1 \pmod{2^2}$ を持ちます．

$x^2 + x + 2 \equiv 0 \pmod{2^2}$ は 2 つの解 $x \equiv 1, 2 \pmod{2^2}$ を持ちます．

$x^2 + 3x + 2 \equiv 0 \pmod{2^2}$ は 2 つの解 $x \equiv 2, 3 \pmod{2^2}$ を持ちます．

$x^2 + x + 1 \equiv 0 \pmod{2^2}$, $x^2 + 3x + 1 \equiv 0 \pmod{2^2}$,
$x^2 + x + 3 \equiv 0 \pmod{2^2}$, $x^2 + 3x + 3 \equiv 0 \pmod{2^2}$ は解を持ちません．

この場合も，2 を法として考えた方程式 $x^2 + ax + b \equiv 0 \pmod{2}$ が 2 つ解を持つときは，2 つの解それぞれが $x^2 + ax + b \equiv 0 \pmod{2^2}$ の解に一意的に持ち上がっていることがわかります．

$\mathrm{mod}\, p^e$ での方程式

さらに，p^e を法とした合同式の世界での方程式の解の個数について
少し考えてみます．

$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ を整数係数の n 次多項式とします．
素数 p を一つ固定して，p^e を法として考えた方程式

$$f(x) \equiv 0 \ (\mathrm{mod}\, p^e)$$

の解の個数を $N(e)$ とするとき，数列

$$N(1), N(2), N(3), ...$$

の振る舞いはどうなっているでしょうか？

数列 $N(1), N(2), N(3), ...$ の母関数と呼ばれる級数

$$P(t) = 1 + N(1)t + N(2)t^2 + N(3)t^3 + \cdots$$

を簡単な例で計算しましょう．

$\mathrm{mod}\, p^e$ での方程式

$f(x) = x^2$ のとき．このときは

$$
\begin{aligned}
& x^2 \equiv 0 \pmod{p^e} \\
\Longleftrightarrow\ & x^2 \text{ が } p \text{ で } e \text{ 回以上割り切れる} \\
\Longleftrightarrow\ & x \text{ が } p \text{ で } \lceil e/2 \rceil \text{ 回以上割り切れる} \\
\Longleftrightarrow\ & x \equiv p^{\lceil e/2 \rceil} a \pmod{p^e} \quad (0 \le a \le p^{e-\lceil e/2 \rceil} - 1)
\end{aligned}
$$

です ($\lceil e/2 \rceil$ は $e/2$ の切り上げ)．従って $N(e) = p^{e-\lceil e/2 \rceil}$, つまり

$$
\begin{aligned}
& N(1) = p^{1-1} = 1, \quad N(2) = p^{2-1} = p, \\
& N(3) = p^{3-2} = p, \quad N(4) = p^{4-2} = p^2, \\
& N(5) = p^{5-3} = p^2, \ldots
\end{aligned}
$$

従って

$$
\begin{aligned}
P(t) &= (1+t) + p(t^2+t^3) + p^2(t^4+t^5) + \cdots \\
&= (1+t)(1+pt^2+p^2t^4+\cdots) = \frac{1+t}{1-pt^2}
\end{aligned}
$$

となります．

$\mathrm{mod}\, p^e$ での方程式

次に，$p \neq 2$ と仮定して$f(x) = x^2 - 1$ のときを考えます．

$$x^2 - 1 \equiv 0 \pmod{p^e} \iff (x+1)(x-1) \equiv 0 \pmod{p^e}$$

ですが，仮定 $p \neq 2$ より $x+1, x-1$ のいずれかは p で割り切れないのでこれは

$$x - 1 \equiv 0 \pmod{p^e} \quad \text{または} \quad x + 1 \equiv 0 \pmod{p^e}$$

であることと同値です．よって $N(e) = 2$ なので，

$$P(t) = 1 + 2t + 2t^2 + 2t^3 + \cdots = 1 + \frac{2t}{1-t} = \frac{1+t}{1-t}$$

となります．

一般の $f(x)$ の場合は難しそうです．次の結果が知られています．

$\mathrm{mod}\, p^e$ での方程式

定理

$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ を整数係数の n 次多項式とする．p^e を法として考えた方程式

$$f(x) \equiv 0 \pmod{p^e}$$

の解の個数を $N(e)$ とし，

$$P(t) = 1 + N(1)t + N(2)t^2 + N(3)t^3 + \cdots$$

とおく．このとき，$P(t)$ は t の有理式 ($\dfrac{\text{多項式}}{\text{多項式}}$ の形の式) になる．

証明？

定理の状況では，方程式を $\mathrm{mod}\, p$, $\mathrm{mod}\, p^2$, $\mathrm{mod}\, p^3$, ... で考えています．
従って，方程式の解を考えるときに，整数において考えるのではなく
『「整数を p で割った余り」，「整数を p^2 で割った余り」, ... の列』の集合
において考える方が自然な感じがします．
(さきほど，$\mathrm{mod}\, p$ で考えた方程式の解を $\mathrm{mod}\, p^2$ に持ち上げようとした
ことを思い出しましょう．)
これが p 進整数と呼ばれるものです．

p 進整数の世界で考えることにより定理が証明されますが，
この講演では定理を眺めるだけにして終わりにしたいと思います．

ありがとうございました！