奥積雅彦（総務省統計研究研修所教官）

統計を理解するための学び直し（その５）　素因数分解

【素因数分解とは】
　本稿では、統計図書館コラム【雑学編】号外（統計史料でみる昭和・平成期【その３】＋令和期 附録２）「2021年を振り返るはずが」に関連して、素因数分解について学び直しをしてみました。
　国立国会図書館デジタルコレクションで公開されている戦前の資料で素因数分解について解説している最も古いものを検索したところ、薗村宗太郎 編「新撰普通算術 上巻」（明治 34 年 1901 年）にヒットしました。同書の「整数の性質」のセクションにおける素数、素因数、素因数分解法の定義をここに紹介します。120 年以上前の資料も味わいがあることを実感しました。

（素数） 素数とは本数或は一を除くの外他の数にて約すべからざる数を言う …	
https://dl.ndl.go.jp/pid/827475/1/111　QR コード⇒ （国立国会図書館デジタルコレクション）	
（素因数） 素因数とは其数の因数にして素数なるものを言う （素因数分解法） 素因数分解法とは某数を分解して素因数若干の相乗積に等しきことを明かにする法なり …	
https://dl.ndl.go.jp/pid/827475/1/115　QR コード⇒ （国立国会図書館デジタルコレクション）	
【出典】薗村宗太郎 編「新撰普通算術 上巻」（明治 34 年 1901 年）	

【素因数分解に関する問題】
　インターネットで公開されている素因数分解に関する問題に係る動画のサムネイルをみて、筆者が理解しやすいようにアレンジ、脚色して解いてみましたので紹介します。

問１　素因数分解せよ 3,200,021　ただし素因数は３つである

【解法】
$3{,}200{,}021=20^5+20+1$※

※$3{,}200{,}000=32*10^5=2^5*10^5=20^5$ なので、$3{,}200{,}021=20^5+20+1$ を想起

$x^5+x+1=x^5-x^2+x^2+x+1$
$=x^2(x^3-1)+x^2+x+1$
$=x^2(x-1)(x^2+x+1)+x^2+x+1$
$=(x^2+x+1)(x^3-x^2+1)$

$20^5+20+1=(20^2+20+1)(20^3-20^2+1)$
$=(400+20+1)(8{,}000-400+1)=421*7{,}601$【参考】
$=421*691*11$【参考】$=11*421*691$

　11 は素数。421 は、$\sqrt{421}$以下の素数（2,3,5,7,11,13,17,19）で割り切れないことから素数。691 は、$\sqrt{691}$以下の素数（2,3,5,7,11,13,17,19,23）で割り切れないことから素数。
　よって、$3{,}200{,}021=11*421*691$

【参考】ちなみに、偶数の桁の和と奇数の桁の和との差が 11 の倍数又は 0 であれば、その数は 11 の倍数であるので、7,601 は、11 で割り切れます。また、691*11 は、和（a+b=691）と差（a-b=11）の積と想定し、a、b を求めると、 a＝351、b＝340。よって、691*11＝(351+340)(351-340)=123,201-115,600=7,601

問２　1,280,000,401 を素因数分解した時の素因数を１つ求めよ

【解法】
$1{,}280{,}000{,}401=20^7+20^2+1$※

※$1{,}280{,}000{,}000=128*10^7=32*4*10^7=2^5*2^2*10^7=2^7*10^7=20^7$ なので、$1{,}280{,}000{,}401=20^7+20^2+1$ を想起

$x^7+x^2+1=x^7+x^3+x^2-x^3-x^2-x+x^2+x+1$
$=x^2(x^5+x+1)-x(x^2+x+1)+(x^2+x+1)$
$=x^2(x^2+x+1)(x^3-x^2+1)-x(x^2+x+1)+(x^2+x+1)$
$=(x^2+x+1)(x^2(x^3-x^2+1)-x+1)=(x^2+x+1)(x^5-x^4+x^2-x+1)$

20^7+20^2+1
$=(20^2+20+1)(20^2(20^3-20^2+1)-20+1)$
$=421(20^5-20^4+20^2-20+1)$
$=421(3{,}200{,}000-160{,}000+400-20+1)$
$=421\times3{,}040{,}381$

421 は、$\sqrt{421}$以下の素数（2,3,5,7,11,13,17,19）で割り切れないことから素数。
よって、1,280,000,401 を素因数分解したときの素因数の１つは 421

問３　2,501 を素因数分解せよ

【解法 1】
2,501 を和と差の積の形に因数分解できないかみてみる。
$50^2=2{,}500\rightarrow2{,}500-2{,}501=-1\rightarrow$手詰まり
$51^2=2{,}601\rightarrow2{,}601-2{,}501=100\rightarrow2{,}501=51^2-10^2=(51+10)(51-10)=61*41$
41 は$\sqrt{41}$以下の素数(2,3,5)で割り切れないことから素数。
61 は$\sqrt{61}$以下の素数(2,3,5,7)で割り切れないことから素数。
よって、2501=41*61

【解法 2】
2501 を x^2+1 にあてはめると
50^2+1
$x^2+1=(x+1)^2-2x$ なので
$50^2+1=51^2-2*50=51^2-10^2=(51+10)(51-10)=61*41$
41 と 61 は解法 1 でみたとおりいずれも素数。
よって、2501=41*61

【解法 3】
2501 を $4x^4+1$ にあてはめると
$4*5^4+1$
$4x^4+1=(2x^2+1)^2-(2x)^2=(2x^2+1+2x)(2x^2+1-2x)$なので
$4*5^4+1=(2*5^2+1+2*5)(2*5^2+1-2*5)=(51+10)(51-10)=61*41$
41 と 61 は解法 1 でみたとおりいずれも素数。
よって、2501=41*61

問４　40,001 を素因数分解せよ

【解法 1】
40001 を和と差の積の形に因数分解できないかみてみる。
$200^2=40{,}000\rightarrow40{,}000-40{,}001=-1\rightarrow$手詰まり
$201^2=40{,}401\rightarrow40{,}401-40{,}001=400\rightarrow40{,}001=201^2-20^2=(201+20)(201-20)=221*181$
181 は$\sqrt{181}$以下の素数(2,3,5,7,11,13)で割り切れないことから素数
221 は$\sqrt{221}$以下の素数(2,3,5,7,11,13)で割り切れるか順次みていくと 13(素数)で割り切れる。→221 を 13 で割ると商は 17(素数)。(あるいは $221=225-4=15^2-2^2=(15+2)(15-2)=17*13$ →13 と 17 はいずれも素数)
よって、40,001=13*17*181

【解法 2】
40,001 を x^2+1 にあてはめると
200^2+1
$x^2+1=(x+1)^2-2x$ なので
$200^2+1=(201)^2-2*200=(201)^2-20^2=(201+20)(201-20)=221*181$
解法 1 でみたとおり、181 は素数で、221 は 13*17(いずれも素数)
よって、40,001=13*17*181

【解法 3】
40,001 を $4x^4+1$ にあてはめると
$4x^4+1=(2x^2+1)^2-(2x)^2=(2x^2+1+2x)(2x^2+1-2x)$なので
$(2*10^2+1+2*10)(2*10^2+1-2*10)=(201+20)(201-20)=221*181$
解法 1 でみたとおり、181 は素数で、221 は 13*17(いずれも素数)
よって、40,001=13*17*181

【27,000,001 の素因数分解】
以上のほか、インターネットで公開されている素因数分解に関する問題を探索したところ、次の問題に出会いましたので、筆者が理解しやすいようにアレンジ、脚色して解いてみましたので紹介します。

問　27,000,001 を素因数分解せよ

【解法】
27,000,001 を x^3+1 にあてはめると
$27,000,001=300^3+1$

$x^3+1=(x+1)(x^2-x+1)$なので
$300^3+1=(300+1)(300^2-300+1)$
$=301*89,701$

301 を$\sqrt{301}$以下の素数(2,3,5,7,11,13,17)で小さい数から順に見ていくと 7 で割り切れる。301 を 7 で割ると商は 43。43 は$\sqrt{43}$以下の素数(2,3,5)で割り切れないことから素数。(あるいは $301=625-324=25^2-18^2=(25+18)(25-18)=43*7$ →7 と 43 はいずれも素数)
→301=7*43
次に 89, 701 を和と差の積の形に因数分解できないかみてみる。
$300^2=90,000$→90,000-89,701=299→手詰まり
$301^2=90,601$→90,601-89,701=900→$89,701=301^2-30^2=(301+30)(301-30)=331*271$
271 は$\sqrt{271}$以下の素数(2,3,5,7,11,13)で割り切れないことから素数。
331 は$\sqrt{331}$以下の素数(2,3,5,7,11,13,17)で割り切れないことから素数。
よって、27,000,001=7*43*271*331

【3.1415*10⁴ の素因数分解】
円周率を覚える手がかりを探すため、3.1415*10⁴ の素因数分解を行ってみました。

問　3.1415*10⁴ の素因数分解

【解法】
下一桁が 5 なので、素数 5 で割り切れることから、$3.1415*10^4=5*6,283$
次に 6,283 を和と差の積で表せる数字を探すと、
$80^2=6,400$、6,400-6,283=117→手詰まり
$81^2=6,401$+160=6561、6,561-6,283=278→手詰まり
$82^2=6,404$+320=6724、6,724-6,283=441→6,283=6,724-441=$82^2-21^2=(82+21)(82-21)=103*61$
103 は、$\sqrt{103}$以下の素数(2,3,5,7)で割り切れないことから素数。
61 は、$\sqrt{61}$以下の素数(2,3,5,7)で割り切れないことから素数。
したがって、$3.1415*10^4=5*6,283=5\times61\times103$

【問題から学んだこと】
・小数点以下第 4 位までの円周率
82(π パイプラスワン)と 21(21 世紀)の和と差の積を 2000(20 世紀末)で割ると、円周率を小数点以下第 4 位まで求めることが可能。⇒$(82+21)(82-21)\times5\div10^4=(82+21)(82-21)\div2000=3.1415$

【素因数分解は何に役立つか･･･】
桁の大きい数の素因数分解の困難さは、暗号化に役立ち、スーパーコンピュータでさえ桁の大きい数の素因数分解が苦手とされているそうです。なお、素因数分解を苦手としない量子コンピュータを意識した、データの新たな暗号化技術も開発されているようです。今後とも情報通信技術は進化し、その開発は、データの新たな暗号化技術の開発と表裏一体･･･でなければならないように思います。
いずれにしても、素因数分解は暗号化のためにのみあるものではありません。素因数分解は、何に役立つかにとどまらず、人類が未知のものに挑戦するツールの一つでもあると思います。ちなみに、共通項（文字、数字、式）でくくる因数分解は、意識・無意識にかかわらず、日常生活で普通に行われています。