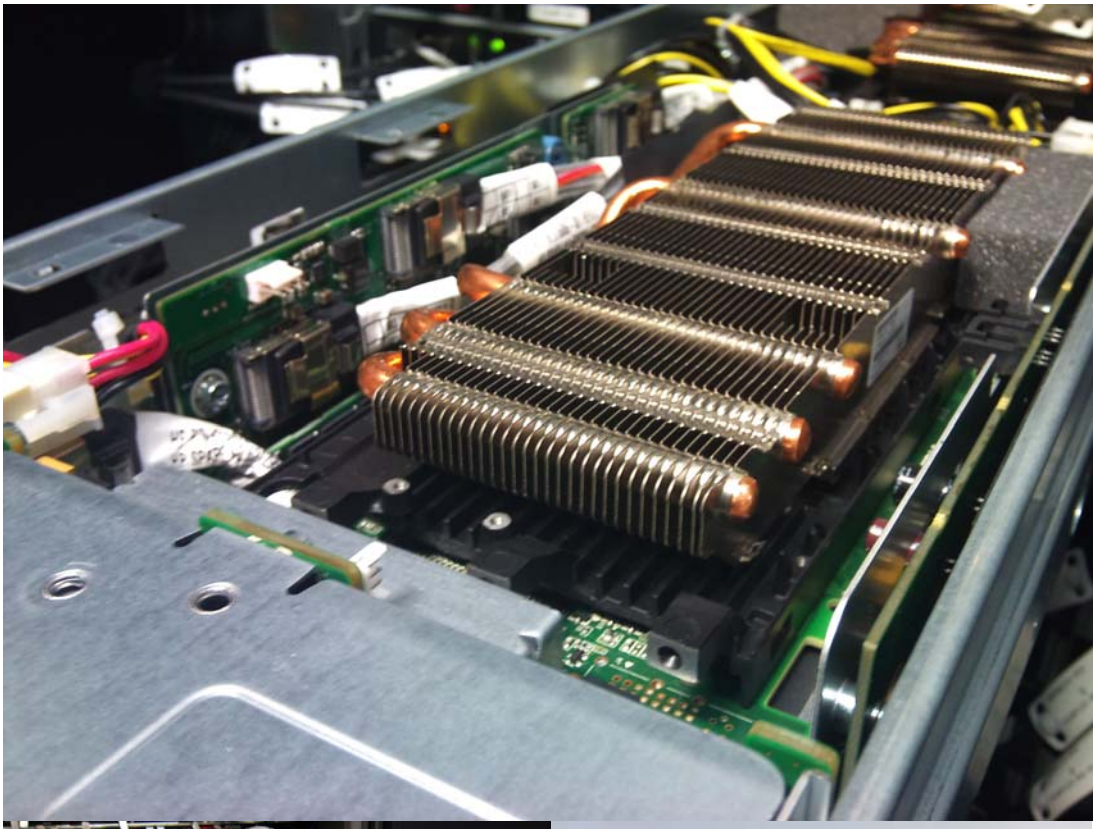
ユークリッドからインターネットそしてスーパーコンピュータへ

住井 英二郎
東北大学大学院情報科学研究科 准教授



右下：今年６月・11 月の２回連続で「TOP500」ランキング世界１位となったスーパーコンピュータ「京」外観（出典 riken.jp）
上および左下：同世界５位のスーパーコンピュータ「TSUBAME2」内部（東京工業大学学術国際情報センター提供）

パソコン少年

小さいころから算数や数学が好きでした。兄がやっていた公〇式を見て、親にせがんで私もやらせてもらいました（小学四年生ぐらいで飽きてやめてしまいましたが）。

小学一年生のとき、兄の中学入学祝いにパソコンを買うというので、一緒にN社のショールームやパソコンショップに連れていってもらいました。今と違って、当時のパソコンは自分でプログラムを書いて使うのが普通でした。子供なので大したことはありませんでしたが、ショールームに通い詰めて、ごく簡単なプログラムは書けるようになりました。

家にパソコンが来てからも、親に「パソコンは一日３０分まで」と制限されてしまったので、紙の上にプログラムを書いて、（紙の上で）実行したりしていました。

当時の一般的な家庭用パソコンはＣＰＵが８ビット・４メガヘルツ程度、メモリは１６キロバイト程度、グラフィックス画面は２５６×１９２ドット程度でした。

現在のＰＣはＣＰＵが６４ビット・２ギガヘルツ（＝２千メガヘルツ）、メモリは２ギガバイト（＝２百万キロバイト）、画面は１９２０×１０８０ドットぐらいでしょうか。それぞれ何倍に増えたか計算してみてください。

フラクタル図形

中学校入学時に私も最新の１６ビットパソコンを買ってもらい、フロッピーディスクが使えるようになったので（それまでは使わせてもらえず、カセットテープにセーブしていました）、それまでより難しいプログラムも書けるようになってきました（依然として一日３０分の制限はありましたが）。

特に、パソコン雑誌で見かけた「フラクタル図形」（自己相似形）を描くプログラムに感動し、自分も書きたくなりました。

しかし、フラクタル図形を描くプログラムは「再帰」という仕組みを使って書かれることが多く、当時の「ＢＡＳＩＣ」というプログラミング言語では書くことができませんでした（他の言語のコンパイラやインタプリタは高価で買えませんでした）。

仕方がないので「再帰」のかわりに「スタック」と呼ばれる仕組みをＢＡＳＩＣの上に作り、それを用いて「再帰」をシミュレートすることにより、何とかフラクタル図形を描くプログラムを書くことに成功しました。

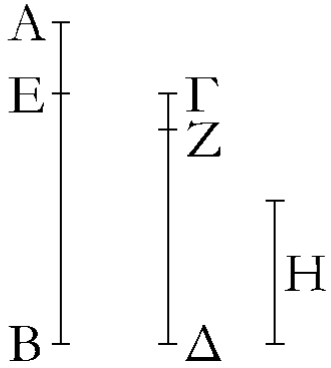
ユークリッドの「原論」

それからしばらく、高校生の間はパソコンよりも純粋数学に興味

Eijiro Sumii
●1975 年東京都生まれ。東京大学理学部情報科学科卒業。同大学院情報理工学研究科コンピュータ科学専攻、ペンシルバニア大学を経て 2005 年東北大学へ。

β΄.

Δύο ἀριθμῶν δοθέντων μὴ πρώτων πρὸς ἀλλήλους τὸ μέγιστον αὐτῶν κοινὸν μέτρον εὑρεῖν.



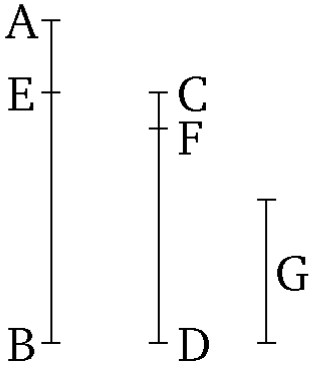
Ἔστωσαν οἱ δοθέντες δύο ἀριθμοὶ μὴ πρῶτοι πρὸς ἀλλήλους οἱ AB, ΓΔ. δεῖ δὴ τῶν AB, ΓΔ τὸ μέγιστον κοινὸν μέτρον εὑρεῖν.

Εἰ μὲν οὖν ὁ ΓΔ τὸν AB μετρεῖ, μετρεῖ δὲ καὶ ἑαυτόν, ὁ ΓΔ ἄρα τῶν ΓΔ, AB κοινὸν μέτρον ἐστίν. καὶ φανερόν, ὅτι καὶ μέγιστον· οὐδεὶς γὰρ μείζων τοῦ ΓΔ τὸν ΓΔ μετρήσει.

Εἰ δὲ οὐ μετρεῖ ὁ ΓΔ τὸν AB, τῶν AB, ΓΔ ἀνθυφαιρουμένου ἀεὶ τοῦ ἐλάσσονος ἀπὸ τοῦ μείζονος λειφθήσεταί τις ἀριθμός, ὃς μετρήσει τὸν πρὸ ἑαυτοῦ. μονὰς μὲν γὰρ οὐ λειφθήσεται· εἰ δὲ μή, ἔσονται οἱ AB, ΓΔ πρῶτοι πρὸς ἀλλήλους· ὅπερ οὐχ ὑπόκειται. λειφήσεταί τις ἄρα ἀριθμὸς, ὃς μετρήσει τὸν πρὸ ἑαυτοῦ. καὶ ὁ μὲν ΓΔ τὸν BE μετρῶν λειπέτω ἑαυτοῦ ἐλάσσονα

Proposition 2

To find the greatest common measure of two given numbers (which are) not prime to one another.



Let AB and CD be the two given numbers (which are) not prime to one another. So it is required to find the greatest common measure of AB and CD.

In fact, if CD measures AB, CD is thus a common measure of CD and AB, (since CD) also measures itself. And (it is) manifest that (it is) also the greatest (common measure). For nothing greater than CD can measure CD.

But if CD does not measure AB then some number will remain from AB and CD, the lesser being continually subtracted, in turn, from the greater, which will measure the (number) preceding it. For a unit will not be left. But if not, AB and CD will be prime to one another [Prop. 7.1]. The very opposite thing was assumed. Thus,

図１：ユークリッド「原論」（紀元前 300 年頃）第７巻命題２より。「世界最古のアルゴリズム」と言われる「ユークリッドの互除法」。現代的に述べると「二つの正整数 m, n の最大公約数を求めるためには、大きいほうの整数を、小さいほうの整数で割っていく。これを互いに繰り返し、小さいほうの整数が大きいほうの整数を割り切ったならば、それが元の m, n の最大公約数となる。」　ただし m, n といった「変数」は 16 世紀末に考えられたため、「原論」では変数ではなく線分を用いて整数を表している。プログラム（例えば C 言語の関数）で書くと gcd(m,n){return(n==0?m:gcd(n,m%n));}のようになる。

```
> cd openssl-1.0.0e/crypto/
> grep euclid bn/bn_gcd.c
static BIGNUM *euclid(BIGNUM *a, BIGNUM *
b);
t=euclid(a,b);
static BIGNUM *euclid(BIGNUM *a, BIGNUM *
b)
> grep gcd rsa/*.c
rsa/rsa_chk.c:
r = BN_gcd(m, i, j, ctx);
rsa/rsa_gen.c:
if (!BN_gcd(r1,r2,rsa->e,ctx)) goto err;
rsa/rsa_gen.c:
if (!BN_gcd(r1,r2,rsa->e,ctx)) goto err;
```

図２：HTTPS など、インターネット上の安全な暗号化通信を実現するプログラムの一部。実際に「ユークリッド(Euclid)の互除法」により、巨大な整数(big num)の最大公約数(greatest common divisor)を計算している。

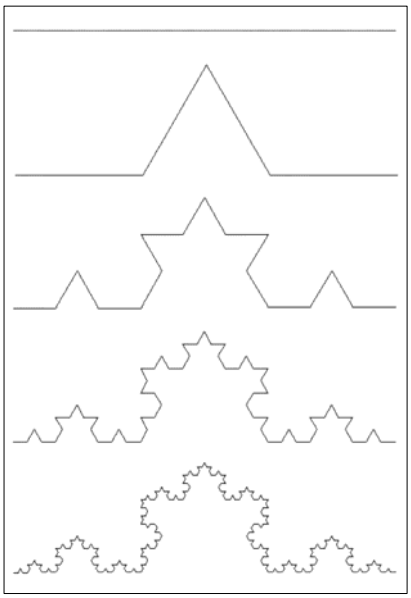


図３：「フラクタル図形」の一種「コッホ曲線」の生成過程。一つの線分（一番上）を三等分し、真ん中の線分を、それを一辺とする正三角形の他の二辺で置き換える（二番目）。この「三等分して真ん中を置き換える」操作を、各線分に対して繰り返す（三番目以降）。プログラムで書くと

```
koch(x) {
  if (x<10) forward(x);
  else {
    koch(x/3);
    left(60); koch(x/3);
    right(120); koch(x/3);
    left(60); koch(x/3);
  }
}
```

ただし forward(x)は「前に長さ x の線分を描いて進む」、left(60)は「左に 60°向きを変える」、right(120)は「右に 120°向きを変える」動作を表す。

スパコン世界１位

時代は一気に下って２００９年１１月、「２位じゃダメなんでしょうか」で有名な「事業仕分け」により、皮肉にも「スーパーコンピュータ」などという用語が世間やマスコミをにぎわせる状況となりました。

その後、まさにその事業仕分けの対象となった「京」がスーパーコンピュータの世界ランキング「ＴＯＰ５００」でダントツ１位を獲得、先月のＴＯＰ５００でも２回連続で１位を獲得しました。

また、同じく日本のスーパーコンピュータ「ＴＳＵＢＡＭＥ２」も２回連続で５位を獲得、両者は他にもスーパーコンピュータ関連の賞を総なめしています。

が移り、「ブルバキ」という２０世紀フランスの数学者グループが書いた「数学原論」という本を読もうとして最初の１章で挫折したり、数学オリンピックの一次予選に落ちたりして（東京の国立高校だったので、周りには本選金メダリストも何人かいました）、自分には数学の才能がない（笑）と考えるようになりました。

ちなみにブルバキの「数学原論」は２０世紀の本ですが、紀元前古代ギリシャの数学者ユークリッドが編纂した「原論」という本に因んだタイトルです。ユークリッドの「原論」には「世界最初のアルゴリズム」と呼ばれる「ユークリッドの互除法」が記されており（図１）、現代のインターネットにおける安全な暗号化通信に欠かせないアルゴリズムとなっています（図２）。