Pinter Consulting
New Series Nos. 11.

J K Pinter, Dr.Tech.

March 29, 2016

Motto

- Meg(g)y? Nem meg(g)y?
- Meg(g)y, de néha eröltetni kell az igényes matematikai továbbképzést.

Előszó

Dr. No hátán az ötös szám jelezte, hogy a jobbfedezet posztját tölti be, de ezen kívül alig emlékeztetett futballistára. Egyik lábán rövid nylonzoknit viselt és kalucsnit, a másikon vastag hegymászó harisnyát és papucsot, de még ennél is jobban megdöbbentett, hogy egy literes üvegben Hubertus likőrt hozott magával, az üveget az öntöző csatorna vízzel telt vaskalitkájába tette, nehogy a tűző napon átmelegedjen, utána felemelt kézzel játékra jelentkezett.

- - - -

Introduction

Pinter Consulting of Calgary, Alberta practices Mathematics, promotes clear thinking and offers Consultations, Tutorials and Seminars in Mathematics.

Contents

Chapter 12

Proceedings

12.1 Summary of Current Report

- **Private study for professional development:**
- Records of activities at Pinter Consulting
- Collection of problems with our own solutions .
- Continuous improvement, corrections and last revisionMarch 29, 2016.

12.2 Tutorial 1.

- Calculus
- *Spartan Old School*
- Last revision March 29, 2016

Exercises

46.

$$\lim_{n \to \infty} \frac{10000n}{n^2+1} = 0.$$

Proof:

$$0 \leq \frac{10000n}{n^2+1} = \frac{10000}{n+\frac{1}{n}} \leq \frac{10000}{n}$$

$$0 \leq \lim_{n \to \infty} \frac{10000n}{n^2+1} \leq \lim_{n \to \infty} \frac{10000}{n} = 0.$$

47.

$$\lim_{n \to \infty} \left(\sqrt{n+1} - \sqrt{n}\right) = 0.$$

Proof:

$$\left(\sqrt{n+1} - \sqrt{n}\right) = \frac{\left(\sqrt{n+1} - \sqrt{n}\right)\left(\sqrt{n+1} + \sqrt{n}\right)}{\left(\sqrt{n+1} + \sqrt{n}\right)}$$

$$= \frac{1}{\left(\sqrt{n+1} + \sqrt{n}\right)}$$

$$\frac{1}{2\sqrt{n+1}} < \frac{1}{\sqrt{n+1} + \sqrt{n}} < \frac{1}{2\sqrt{n}}$$

$$\lim_{n \to \infty} \frac{1}{2\sqrt{n+1}} = \lim_{n \to \infty} \frac{1}{2\sqrt{n}} = 0.$$

49.

$$\lim_{n\to\infty} \frac{(-2)^n + 3^n}{(-2)^{n+1} + 3^{n+1}} = \frac{1}{3}.$$

$$\frac{(-2)^n + 3^n}{(-2)^{n+1} + 3^{n+1}} = \frac{\left[\left(\frac{-2}{3}\right)^n + 1\right] 3^n}{\left[\left(\frac{-2}{3}\right)^{n+1} + 1\right] 3^{n+1}} = \frac{\left[\left(\frac{-2}{3}\right)^n + 1\right]}{\left[\left(\frac{-2}{3}\right)^{n+1} + 1\right]} \times \frac{1}{3}$$

$$\lim_{n\to\infty} \frac{\left[\left(\frac{-2}{3}\right)^n + 1\right]}{\left[\left(\frac{-2}{3}\right)^{n+1} + 1\right]} = 1.$$

48.

$$\lim_{n\to\infty} \frac{n^{\frac{2}{3}} \sin(n!)}{n+1} = 0$$

Proof:

$$|\sin(n!)| \leq 1$$

$$\left|\frac{n^{\frac{2}{3}} \sin(n!)}{n+1}\right| \leq \left|\frac{n^{\frac{2}{3}}}{n+1}\right| |\sin(n!)| \leq \left|\frac{n^{\frac{2}{3}}}{n+1}\right| \leq \left|\frac{n^{\frac{-1}{3}}}{1+n^{-1}}\right| \leq \left|n^{\frac{-1}{3}}\right|$$

$$\lim_{n\to\infty} \left|n^{\frac{-1}{3}}\right| = 0.$$

50.

$$\lim_{n\to\infty} \frac{1 + a + a^2 + a^3 + \ldots + a^n}{1 + b + b^2 + b^3 + \ldots + b^n} = \frac{1-b}{1-a}; \ (|a| < 1, |b| < 1)$$

Proof:

$$1 + a + a^2 + a^3 + \ldots + a^n = \frac{a^{n+1} - 1}{a - 1} = \frac{1 - a^{n+1}}{1 - a} \Longrightarrow \frac{1}{1-a}; \ n \to \infty$$

$$1 + b + b^2 + b^3 + \ldots + b^n = \frac{b^{n+1} - 1}{b - 1} = \frac{1 - b^{n+1}}{1 - b} \Longrightarrow \frac{1}{1-b}; \ n \to \infty$$

$$\lim_{n\to\infty} \frac{1 - a^{n+1}}{1 - a} \frac{1 - b}{1 - b^{n+1}} = \frac{1-b}{1-a}.$$

51.

$$\lim_{n\to\infty}\left(\frac{1}{n^2}+\frac{2}{n^2}+\ldots+\frac{n-1}{n^2}\right)=\frac{1}{2}$$

Proof:

$$1+2+3+\ldots+(n-1)=\frac{(n-1)n}{2}=\frac{n^2-n}{2}$$

$$\lim_{n\to\infty}\frac{n^2-n}{2n^2}=\lim_{n\to\infty}\frac{1-\frac{1}{n}}{2}=\frac{1}{2}.$$

52.

$$\lim_{n\to\infty}\left|\frac{1}{n}-\frac{2}{n}+\frac{3}{n}-\ldots+\frac{(-1)^{n-1}n}{n}\right|=\frac{1}{2}$$

Proof:

$$\begin{aligned}1-2+3 &= +2\\ 1-2+3-4 &= -2\\ 1-2+3-4+5 &= +3\\ 1-2+3-4+5-6 &= -3\\ &\vdots\\ 1-2+3-4+5+\ldots+(2n-1) &= +n\\ 1-2+3-4+5+\ldots\ldots\ldots-2n &= -n\end{aligned}$$

$$\frac{1}{n}-\frac{2}{n}+\frac{3}{n}-\ldots+\frac{(-1)^{n-1}n}{n}=\begin{cases}\dfrac{n}{2n-1}\\ \dfrac{-n}{2n}\end{cases}$$

$$\left|\frac{n}{2n-1}\right|\Longrightarrow\frac{1}{2};\quad\left|\frac{-n}{2n}\right|\Longrightarrow\frac{1}{2};\quad n\to\infty.$$

53.

$$\lim_{n\to\infty} \left[\frac{1^2}{n^3} + \frac{2^2}{n^3} + \frac{3^2}{n^3} + \ldots + \frac{(n-1)^2}{n^3}\right] = \frac{1}{3}.$$

Proof:

$$1^2 + 2^2 + 3^2 + \ldots + (n-1)^2 = \frac{(n-1)(n)(2n-1)}{6} = \frac{2n^3 + O(n^2)}{6}$$

$$\lim_{n\to\infty} \frac{2n^3 + O(n^2)}{6n^3} = \frac{2}{6} = \frac{1}{3}.$$

54.

$$\lim_{n\to\infty} \left[\frac{1^2}{n^3} + \frac{3^2}{n^3} + \frac{5^2}{n^3} + \ldots + \frac{(2n-1)^2}{n^3}\right] = \frac{4}{3}.$$

Proof:

$$1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \frac{n(4n^2-1)}{3} = \frac{4n^3 + O(n)}{3}$$

$$\lim_{n\to\infty} \frac{4n^3 + O(n)}{3n^3} = \frac{4}{3}.$$

Remarks:

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

$$1^2 + 3^2 + 5^2 \ldots + (2n-1)^2 = \frac{n(4n^2-1)}{3}$$

For proofs by induction see *Tutorials on Higher Arithmetic.*

55.

$$\lim_{n \to \infty} \left(\frac{1}{2} + \frac{3}{2^2} + \frac{5}{2^3} + \ldots + \frac{2n-1}{2^n}\right) = 3.$$

Proof: Consider the following triangular arrangement:

$$\begin{array}{llllllll}
\frac{1}{2} & & & & & & & \frac{1}{2} \\
\frac{1}{4} & \frac{1}{4} & \frac{1}{4} & & & & & \frac{3}{2^2} \\
\frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & & & \frac{5}{2^3} \\
\frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{7}{2^4} \\
\ldots & \ldots & \ldots & \ldots & & & & \ldots
\end{array}$$

First column

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \ldots = 1.$$

Second and third

$$\frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \ldots = \frac{1}{2}; \ \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \ldots = \frac{1}{2}.$$

Fourth and fifth

$$\frac{1}{8} + \frac{1}{16} + \ldots = \frac{1}{4}; \ \frac{1}{8} + \frac{1}{16} + \ldots = \frac{1}{4} \quad \text{etc.}$$

$$1 + (\frac{1}{2} + \frac{1}{2}) + (\frac{1}{4} + \frac{1}{4}) + (\frac{1}{8} + \frac{1}{8}) + \ldots = 1 + 1 + \frac{1}{2} + \frac{1}{4} + \ldots = 3.$$

56.

$$\lim_{n \to \infty} \left(\frac{1}{1*2} + \frac{1}{2*3} + \frac{1}{3*4} + \ldots + \frac{1}{n*(n+1)}\right) = 1.$$

Proof:

$$\begin{aligned}
a_n &= \frac{1}{1*2} + \frac{1}{2*3} + \frac{1}{3*4} + \ldots + \frac{1}{n*(n+1)} \\
&= \frac{2-1}{1*2} + \frac{3-2}{2*3} + \frac{4-3}{3*4} + \ldots + \frac{(n+1)-n}{n*(n+1)}
\end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{2}{1*2} - \frac{1}{1*2}\right) + \left(\frac{3}{2*3} - \frac{2}{2*3}\right) + \left(\frac{4}{3*4} - \frac{3}{3*4}\right) + \dots \\
&+ \left(\frac{n+1}{n*(n+1)} - \frac{n}{n*(n+1)}\right) \\
&= 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \dots + \frac{1}{n} - \frac{1}{n+1} \\
&= 1 - \frac{1}{n+1}.
\end{aligned}
$$

$$\lim_{n \to \infty} a_n = 1.$$

57.

$$\lim_{n \to \infty} \sqrt{2}\sqrt[4]{2}\sqrt[8]{2}\dots\sqrt[2n]{2} = 2.$$

Proof:

$$
\begin{aligned}
a_n &= \sqrt{2}\sqrt[4]{2}\sqrt[8]{2}\dots\sqrt[2n]{2} \\
\ln a_n &= \frac{1}{2}\ln 2 + \frac{1}{4}\ln 2 + \frac{1}{8}\ln 2 + \dots + \frac{1}{2^n}\ln 2 \\
&= \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots + \frac{1}{2^n}\right)\ln 2
\end{aligned}
$$

$$\lim_{n \to \infty} \ln a_n = \ln 2.$$

58.

$$\lim_{n \to \infty} \frac{n}{2^n} = 0.$$

Proof:

$$
\begin{aligned}
n &> 1 \\
\frac{n}{2^{(n+1)}} &> \frac{1}{2^{(n+1)}} \\
\frac{n}{2^{(n+1)}} + \frac{n}{2^{(n+1)}} &> \frac{n}{2^{(n+1)}} + \frac{1}{2^{(n+1)}} \\
\frac{n}{2^n} &> \frac{n+1}{2^{n+1}}
\end{aligned}
$$

Therefore $\frac{n}{2^n}$ is strictly monotone decreasing. Further, let us examine

$$2^k > 2k; \quad k > 2.$$

The inequality holds for $k = 3$ $(8 > 4)$. Suppose it is true for some $k \geq 3$, then since

$$2 > \frac{k+1}{k}, \quad \forall k > 2$$

$$2 * 2^k > 2k * \frac{k+1}{k},$$

$$2^{k+1} > 2 * (k+1).$$

Therefore the inequality is true for all $k > 3$. Now let us choose a small positve number $\varepsilon < \frac{1}{2^3}$. Then $\exists k$ such that $\frac{1}{2^k} \geq \varepsilon > \frac{1}{2^{k+1}}$. Write $N = N(\varepsilon) = 2^{k+1}$. Next, we show that $\frac{N}{2^N} < \varepsilon$ by the above inequality. Indeed,

$$\frac{N}{2^N} \leq \frac{2^{k+1}}{2^{2^{k+1}}} < \frac{2^{k+1}}{2^{2*(k+1)}} < \frac{2^{k+1}}{2^{(k+1)+(k+1)}} = \frac{1}{2^{(k+1)}} < \varepsilon.$$

Since $\frac{n}{2^n}$ is strictly monotone decreasing and positive we have

$$0 < \frac{n}{2^n} < \varepsilon; \ \forall n, \ n > N(\varepsilon).$$

Proof is complete: $\frac{n}{2^n}$ converges to 0 as $n \to \infty$.

12.3 Tutorial 2.

- *Davenport-Guy : Higher Arithmetic*
- *Spartan Old School*
- Last revision: March 29, 2016

Exercises

1.01

$$a)\ 1+2+3+\ldots+n=\frac{n(n+1)}{2}$$

$$1=\frac{1(1+1)}{2}=1.\surd$$

$$1+2=\frac{2(2+1)}{2}=3.\surd$$

$$1+2+3=\frac{3(3+1)}{2}=6.\surd$$

Induction hypothesis:

$$1+2+3+\ldots+n=\frac{n(n+1)}{2}.$$

$$1+2+3+\ldots+n+(n+1)=\frac{n(n+1)}{2}+(n+1)=$$

$$\frac{n(n+1)}{2}+\frac{2(n+1)}{2}=\frac{(n+1)(n+2)}{2}.\surd$$

$$b)\ 1^2+2^2+3^2+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}$$

$$1^2=\frac{1(1+1)(2+1)}{6}=1.\surd$$

$$1^2+2^2=\frac{2(2+1)(4+1)}{6}=5.\surd$$

$$1^2+2^2+3^2=\frac{3(3+1)(6+1)}{6}=14.\surd$$

Induction hypothesis:

$$1^2+2^2+3^2+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

$$1^2+2^2+3^2+\ldots+n^2+(n+1)^2=\frac{n(n+1)(2n+1)}{6}+(n+1)^2=$$

$$\frac{n(n+1)(2n+1)}{6}+\frac{6(n+1)^2}{6}=\frac{(n+1)[n(2n+1)+6(n+1)]}{6}=$$

$$\frac{(n+1)[2n^2+n+6n+6]}{6}=\frac{(n+1)[2n^2+7n+6]}{6}=\frac{(n+1)(n+2)(2n+3)}{6}.\surd$$

$c)$ $(1^3+2^3+3^3+\ldots+n^3)=(1+2+3+\ldots+n)^2$

$$(1^3+2^3+3^3+\ldots+n^3)=\left(\frac{n(n+1)}{2}\right)^2$$

$$(1^3+2^3+3^3+\ldots+n^3)+(n+1)^3=\left(\frac{n(n+1)}{2}\right)^2+(n+1)^3=$$

$$\frac{n^2(n+1)^2}{4}+\frac{4(n+1)^3}{4}=\frac{(n+1)^2}{4}\left(n^2+4n+4\right)=\frac{(n+1)^2}{4}(n+2)^2=$$

$$\left(\frac{(n+1)(n+2)}{2}\right)^2.\surd$$

$d)$ $1+2+2^2+2^3+\ldots+2^{n-1}=2^n-1.$

$S_0=1=2^1-1=1.\surd$

$S_1=1+2=2^2-1=3.\surd$

$S_2=1+2+4=2^3-1=7.\surd$

$S_{n-1}=1+2+2^2+2^3+\ldots+2^{n-1}=2^n-1$

$S_n=1+2+2^2+2^3+\ldots+2^{n-1}+2^n$

$S_n-2*S_{n-1}=1;$

$S_n=2*S_{n-1}+1=2*(2^n-1)+1=2^{n+1}-2+1=2^{n+1}-1.\surd$

1.02 The *Fibonacci numbers* are defined by

$$F_1 = F_2 = 1; F_n = F_{n-1} + F_{n-2},\ n > 2.$$

The first Fibonacci numbers are:

$$\{1, 1, 2, 3, 5, 8, 13, 21, \ldots\}$$

Set $\tau = \dfrac{1+\sqrt{5}}{2}$, ($\tau$ is called the *golden ratio*) and $\sigma = \dfrac{-1}{\tau}$. Show that

i) $F_n < \tau^n$

ii) $F_n = \dfrac{(\tau^n - \sigma^n)}{\sqrt{5}}$

Remark: The *golden ratio* originates in the proportion

$$1 : x = x : (x+1).$$

$$x^2 = x + 1$$

$$x^2 - x - 1 = 0$$

$$x = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2} = \tau,\ \sigma;$$

for

$$\sigma = -\frac{1}{\tau} = -\frac{2}{1+\sqrt{5}} = -\frac{2(1-\sqrt{5})}{(1+\sqrt{5})(1-\sqrt{5})} = -\frac{2(1-\sqrt{5})}{1-5} = \frac{1-\sqrt{5}}{2}.$$

Proof:

$$\tau = \frac{1+\sqrt{5}}{2};\ 3 > \sqrt{5} > 2$$

$$\tau^2 = \frac{(1+\sqrt{5})^2}{4} = \frac{1+2\sqrt{5}+5}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1 + \tau$$

$$\tau^3 = \tau\tau^2 = \left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{3+\sqrt{5}}{2}\right) = 2 + \sqrt{5}.$$

Therefore

$$F_1 < \tau;\; F_2 < \tau^2;\; F_3 < \tau^3.$$

Hypothesis

$$F_{n-2} < \tau^{n-2};\; F_{n-1} < \tau^{n-1}; n \geq 3.$$

Induction

$$F_{n-2} + F_{n-1} < \tau^{n-2} + \tau^{n-1} = \tau^{n-2}(1+\tau) = \tau^{n-2}\left(1 + \frac{1+\sqrt{5}}{2}\right) =$$

$$\tau^{n-2}\left(\frac{3+\sqrt{5}}{2}\right) = \tau^{n-2}\tau^2 = \tau^n.$$

Thus by the recursive definition of Fibonacci numbers

$$F_{n-2} + F_{n-1} = F_n < \tau^n,$$

and Claim i) is proven.

Next, we show

$$F_n = \frac{(\tau^n - \sigma^n)}{\sqrt{5}};\; n = 1, 2.$$

$$F_1 = \left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right)\left(\sqrt{5}\right)^{-1} = 1.\surd$$

$$F_2 = \left(\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right)\left(\sqrt{5}\right)^{-1} =$$

$$= \left(\left(\frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)\right)\left(\left(\frac{1+\sqrt{5}}{2}\right) + \left(\frac{1-\sqrt{5}}{2}\right)\right)\left(\sqrt{5}\right)^{-1} =$$

$$= \left(\frac{1+\sqrt{5}-1+\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}+1-\sqrt{5}}{2}\right)\left(\sqrt{5}\right)^{-1} =$$

$$= \left(\frac{\sqrt{5}+\sqrt{5}}{2}\right)\left(\frac{1+1}{2}\right)\left(\sqrt{5}\right)^{-1} = \left(\sqrt{5}\right)\left(\sqrt{5}\right)^{-1} = 1.\surd$$

Moreover,

$$\sigma^2 = \left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{1-2\sqrt{5}+5}{4} = \frac{6-2\sqrt{5}}{4} = \frac{3-\sqrt{5}}{2} = 1+\sigma,$$

and recall

$$\tau^2 = 1+\tau.$$

Hence

$$F_n = \frac{(\tau^n - \sigma^n)}{\sqrt{5}} = \frac{(\tau^2\tau^{n-2} - \sigma^2\sigma^{n-2})}{\sqrt{5}} = \frac{(\tau+1)\tau^{n-2} - (\sigma+1)\sigma^{n-2}}{\sqrt{5}}$$

$$= \frac{\tau^{n-1} - \sigma^{n-1}}{\sqrt{5}} + \frac{\tau^{n-2} - \sigma^{n-2}}{\sqrt{5}} = F_{n-1} + F_{n-2},$$

which proves Claim ii) for $n \geq 3$.

1.03 Examples of *prime factorization* :

i) N=999

$$\begin{aligned} 999:3 &= 333 \\ 333:3 &= 111 \\ 111:3 &= 37 \\ 37 &= 37 \end{aligned}$$

$$N = 3*3*3*37.$$

ii) N=1001, by *Fermat's method* .

$$31^2 < 1001 < 32^2$$

Searching for a complete square:

$$\begin{aligned} 32^2 - N &= 23 \\ 33^2 - N &= 88 \\ 34^2 - N &= 155 \\ 35^2 - N &= 224 \\ 36^2 - N &= 295 \end{aligned}$$

$$
\begin{aligned}
37^2 - N &= 368 \\
\ldots &= \ldots \\
45^2 - N &= 1024 = 32^2 \\
45^2 - 32^2 &= N.\surd
\end{aligned}
$$

$$N = (45 + 32)(45 - 32) = 77 * 13 = 7 * 11 * 13.$$

iii) N=1729, by *Fermat's method* .

$$41^2 < 1729 < 42^2$$

$$
\begin{aligned}
42^2 - N &= 35 \\
\ldots &= \ldots \\
55^2 - N &= 1296 = 36^2 \\
55^2 - 36^2 &= N.\surd
\end{aligned}
$$

$$N = (55 + 36)(55 - 36) = 91 * 19 = 7 * 13 * 19.$$

iv) N=11111 The smallest prime factor in N (if any) is not greater than $\sqrt{N}$. Thus we consider the primes up to $\sqrt{N} < 106$:

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97
101	103	107	...	...
...	...	...	...	...
...	...	271	...	...

The first prime that divides N is 41.

$$11111 : 41 = 271$$

It turns out that 271 is also a prime, therefore

$$N = 41 * 271.$$

v) N=65,536

$$\begin{aligned} 65,536:2 &= 32,768 \\ 32,768:2 &= 16,384 \\ 16,384:2 &= 8,192 \\ 8,192:2 &= 4,096 \\ 4,096:2 &= 2,048 \\ 2,048:2 &= 1,024 = 2^{10} \end{aligned}$$

$$N = 2^{16}$$

vi) N=6,469,693,230

$$N \equiv 0, \pmod 2, \pmod 5$$

Check for

$$N \equiv 0, \pmod 3$$

$$6+4+6+9+6+9+3+2+3+0 = 48, \; 3|48.$$

Sum of digits is divisible by 3.
Check for

$$N \equiv 0, \pmod{11}.$$

$$N = \sum_{j=0}^{j=k} a_j * 10^j, \; a_k \neq 0,$$

where

$$a_k a_{k-1} \dots a_0$$

are the digits of number N in conventional 10-based number system.

$$10^0 \equiv 10^2 \equiv \dots \equiv 1, \pmod{11},$$

$$10^1 \equiv 10^3 \equiv \dots \equiv -1, \pmod{11},$$

alternating with odd and even powers.

$$N \equiv a_0 - a_1 + a_2 \ldots \pm a_k, \pmod{11}$$

$$N \equiv (0+2+9+9+4) - (3+3+6+6+6) \pmod{11}$$

$$N \equiv 24 - 24 \equiv 0 \pmod{11}.$$

N is divisible by $2, 3, 5, 11$, all primes.

$$2 * 3 * 5 * 11 = 330$$

$$6,469,693,230 \div 330 = 19,605,131$$

Next, we split $19,605,131$ by *Fermat's method*:

$$4,427^2 < 19,605,131 < 4,428^2$$

$$4,434^2 - 19,605,131 = 55,225 = 235^2$$

$$(4,434 + 235)(4,434 - 235) = 4,669 * 4,199 = 19,605,131$$

The by *trial division*

$$4669 = 7 * 23 * 29, \quad 4199 = 13 * 17 * 19$$

$$6,469,693,230 = 2 * 3 * 5 * 7 * 11 * 13 * 17 * 19 * 23 * 29$$

1.04. *Consecutive composite numbers.* The following series has $(N-1)$ consecutive composite numbers:

$$N! + 2, N! + 3, \ldots N! + (N-1), N! + N$$

because

$$2|N! + 2,\ 3|N! + 3, \ldots (N-1)|N! + (N-1),\ N|N! + N$$

Find 5 consecutive numbers.

$$2|6! + 2,\ 3|6! + 3,\ 4|6! + 4,\ 5|6! + 5,\ 6|6! + 6$$

but

$$24, 25, 26, 27, 28$$

is a sequence of much smaller numbers.

1.05.

$$n^2 + n + 41, \quad n = 0, 1, 2, \ldots$$

Does this formula always give prime numbers ? No, see $n = 40$, $n = 41$.

n	$n^2 + n + 41$
0	41
1	43
2	47
3	53
4	61
5	71
6	83
$\vdots$	$\vdots$
11	173
12	197
13	223
$\vdots$	$\vdots$
20	461
$\vdots$	$\vdots$
39	1601
40	$1681 = 41 * 41$
41	$1763 = 41 * 43$
42	1847
$\vdots$	$\vdots$
53	2903

Numbers checked in *Table of Primes.*

1.06. *Express* 22! *as a product of prime factors.*

Let p be a prime number. Then the exact power of p that divides $n!$ is given by

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

where there are only finite number of non-zero terms in the series. Then

$$n! = 1 \cdot 2 \cdots (p-1) \cdot p \cdot (p+1) \cdots p^2 \cdots$$

and there are $\left[\dfrac{n}{p}\right]$ that are divisible by p, out of these there are $\left[\dfrac{n}{p^2}\right]$ divisible by p^2; moreover, the multiples of p^3 number $\left[\dfrac{n}{p^3}\right]$ etc. We continue until we reach p^m where m is the highest power of p contained in n. Take $p = 2$,

$$2^4 < 22 < 2^5$$

$$\left[\frac{22}{2}\right] + \left[\frac{22}{2^2}\right] + \left[\frac{22}{2^3}\right] + \left[\frac{22}{2^4}\right] + \left[\frac{22}{2^5}\right] \ldots =$$

$$[11] + [5.5] + [2.75] + [1.375] + [0.6875] =$$

$$11 + 5 + 2 + 1 + 0 = 19.$$

Next, $p = 3$

$$3^2 < 22 < 3^3$$

$$\left[\frac{22}{3}\right] + \left[\frac{22}{3^2}\right] + \left[\frac{22}{3^3}\right] + \ldots =$$

$$[7.3333] + [2.4444] + [0.8148] = 7 + 2 + 0 = 9.$$

For the other primes $p = 5, 7, 11, 13, 17, 19$, less than 22 we have

$$\left[\frac{22}{5}\right] = 4; \quad \left[\frac{22}{5^2}\right] = \left[\frac{22}{5^3}\right] = \ldots = 0$$

$$\left[\frac{22}{7}\right] = 3; \quad \left[\frac{22}{7^2}\right] = \left[\frac{22}{7^3}\right] = \ldots = 0$$

$$\left[\frac{22}{11}\right] = 2; \quad \left[\frac{22}{11^2}\right] = \left[\frac{22}{11^3}\right] = \ldots = 0$$

$$\left[\frac{22}{13}\right] = \left[\frac{22}{17}\right] = \left[\frac{22}{19}\right] = 1$$

$$\left[\frac{22}{13^2}\right] = \left[\frac{22}{17^2}\right] = \left[\frac{22}{19^2}\right] = 0$$

Therefore

$$22! = 2^{19} \times 3^9 \times 5^4 \times 7^3 \times 11^2 \times 13 \times 17 \times 19.$$

Check:

$$\begin{aligned} 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 &\quad \times \\ 12 \times 13 \times 14 \times 15 \times 16 \times 17 \times 18 \times 19 \times 20 \times 21 \times 22 &\quad = \\ 2^{19} \times 3^9 \times 5^4 \times 7^3 \times 11^2 \times 13 \times 17 \times 19. & \end{aligned}$$

$$\begin{aligned} 1 \times 2 \times 3 \times 2^2 \times 5 \times (2*3) \times 7 \times 2^3 &\quad \times \\ 3^2 \times (2*5) \times 11 \times (3*2^2) \times 13 \times (2*7) \times (3*5) &\quad \times \\ (2^4) \times 17 \times (2*3^2) \times 19 \times (2^2*5) \times (3*7) \times (2*11) &\quad = \\ 2^{19} \times 3^9 \times 5^4 \times 7^3 \times 11^2 \times 13 \times 17 \times 19. & \end{aligned}$$

1.07. *Show that, if 2^a is the highest power of 2 which divides $n!$ then a lies between $n-1$ (higher bound) and $n - \lfloor \log_2(n+1) \rfloor$, (lower bound) where $\lfloor \log_2(n+1) \rfloor$ is the exponent of the greatest power of 2 not greater than $n+1$.*

Discussion: Let us take a look at some numbers. The first column contains some integers from $n = 4 = 2^2$ to $n = 16 = 2^4$. The second column shows the factorials, $n!$, one can see how fast they grow.

n	$n!$	$\lfloor \log_2(n+1) \rfloor$	*lower*	a	*upper*	2^a
4	24	2	2	3	3	2^3
5	120	2	3	3	4	2^3
6	720	2	4	4	5	2^4
7	5,040	3	4	4	6	2^4
8	40,320	3	5	7	7	2^7
9	362,880	3	6	7	8	2^7
10	3,628,800	3	7	8	9	2^8
11	39,916,800	3	8	8	10	2^8
12	479,001,600	3	9	10	11	2^{10}
13	6,227,020,800	3	9	10	11	2^{10}
14	87,178,291,200	3	9	10	11	2^{10}
15	1,307,674,368,000	3	9	10	11	2^{10}
16	20,922,789,888,000	4	12	15	15	2^{15}

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2		*		*		*		*		*		*		*		*
4				*				*				*				*
8								*								*
16																*

1.08 *If $p \geq 5$ is prime, show that the sum of products in pairs of the numbers $1, 2, 3 \ldots p-1$ is divisible by p. We do not count $1 * 1$, and $1 * 2$ precludes $2 * 1$.*

First, we demonstrate the claim. Let $p = 5$.

$$S_5 = \frac{1}{2}\Big((1+2+3+4)^2 - (1^2+2^2+3^2+4^2)\Big)$$

$$S_5 = \frac{1}{2}(100-30) = 35, \quad 5|35.$$

Second example, $p = 7$:

$$S_7 = \frac{1}{2}\Big((1+2+3+4+5+6)^2 - (1^2+2^2+3^2+4^2+5^2+6^2)\Big)$$

$$S_7 = \frac{1}{2}\Big(21^2 - 91\Big) = 175, \quad 7|175.$$

Take all possible products then discard the ones we do not want. If $p \geq 5$ is prime, then

$$p \equiv \pm 1, \pmod 3$$

and

$$p = 4k \pm 1, \quad k = 1, 2 \ldots$$

moreover

$$1 + 2 + 3 + \ldots + (p-1) = \frac{p(p-1)}{2}$$

$$1^2 + 2^2 + 3^2 + \ldots + (p-1)^2 = \frac{(p-1)p(2p-1)}{6}.$$

Trivial calculation shows

$$
\begin{aligned}
S_p &= \frac{1}{2}\left(\left(\frac{p(p-1)}{2}\right)^2 - \frac{(p-1)p(2p-1)}{6}\right) \\
&= \frac{1}{2}\left(\frac{p^2(p-1)^2}{2^2} - \frac{(p-1)p(2p-1)}{6}\right) \\
&= \frac{1}{2}\left(\frac{3p^2(p-1)^2}{12} - \frac{2(p-1)p(2p-1)}{12}\right) \\
&= \frac{p}{24}\Big(3p(p-1)^2 - 2(p-1)(2p-1)\Big) \\
&= \frac{p}{24}\Big(3p^3 - 10p^2 + 9p - 2\Big)
\end{aligned}
$$

$p \equiv 1, \pmod 3$

$3p^3 - 10p^2 + 9p - 2 \equiv 3 - 10 + 1 \equiv 0 \pmod 3$

$p \equiv -1, \pmod 3$

$3p^3 - 10p^2 + 9p - 2 \equiv -3 - 10 - 9 - 2 \equiv 0 \pmod 3$

$3 | 3p^3 - 10p^2 + 9p - 2.$

$p = 4k - 1$

$(4k-1)^2 \equiv 1, \pmod 8$

$(4k-1)^3 \equiv (4k-1), \pmod 8$

$$
\begin{aligned}
3(4k-1)^3 - 10(4k-1)^2 + 9(4k-1) - 2 &\equiv \\
3(4k-1) - 10 + 9(4k-1) - 2 &\equiv \\
12(4k-1) - 12 &\equiv 0, \pmod 8
\end{aligned}
$$

$p = 4k + 1$

$(4k+1)^2 \equiv 1, \pmod 8$

$(4k+1)^3 \equiv (4k+1), \pmod 8$

$$\begin{aligned} 3(4k+1)^3 - 10(4k+1)^2 + 9(4k+1) - 2 &\equiv \\ 3(4k+1) - 10 + 9(4k+1) - 2 &\equiv \\ 12(4k+1) - 12 &\equiv 0, \pmod 8 \end{aligned}$$

$8|3p^3 - 10p^2 + 9p - 2.$

$(3,8) = 1$

$24|3p^3 - 10p^2 + 9p - 2.$

Therefore $p|S_p$.

12.4 Tutorial 3.

- *Davenport-Guy : Higher Arithmetic*
- *Spartan Old School*
- Last revision: March 29, 2016

Exercises

1.11 *If $2^n - 1$ is prime, show that n is prime. Is the converse true? (Davenport-Guy)*

Prime numbers of the form $2^n - 1$ are the Mersenne primes. If $2^n - 1$ is prime then n is prime, for suppose to the contrary that $n = kl$ is composite number where k is a proper divisor of n. Then

$$\begin{aligned}
(2^n - 1) &= (2^k - 1)(2^{(l-1)k} + 2^{(l-2)k} + 2^{(l-3)k} \ldots + 1) \\
&= 2^k(2^{(l-1)k} + 2^{(l-2)k} + 2^{(l-3)k} \ldots + 1) \\
&- (2^{(l-1)k} + 2^{(l-2)k} + 2^{(l-3)k} \ldots + 1) \\
&= 2^{lk} + 2^{(l-1)k} + 2^{(l-2)k} \ldots + 2^k \\
&- 2^{(l-1)k} - 2^{(l-2)k} - 2^{(l-3)k} \ldots - 1 \\
&= 2^{lk} - 1,
\end{aligned}$$

so $2^n - 1$ has a proper divisor, $2^k - 1$. Therefore the primality of $2^n - 1$ is reduced to the primality of $2^p - 1$, where p is prime.

Standard notation for Mersenne prime is

$$M_p = 2^p - 1.$$

Hua gives a list of known Mersenne primes (27 numbers). Examples:

$$p = 2, 3, 5, 7, 13$$

$$M_2 = 2(2^2 - 1) = 6$$

$$M_3 = 2^2(2^3 - 1) = 28$$

$$M_5 = 2^4(2^5 - 1) = 496$$

$$M_{13} = 2^{12}(2^{13} - 1) = 4096 * 8191 = 33550336$$

Not all odd primes generate Mersenne primes. Observe that

$$(2^{11} - 1) = 2047 = 23 * 89.$$

Check by Fermat's method:

$$45^2 < 2047 < 46^2$$

$$\begin{aligned}
46^2 - 2047 &= 69 \\
47^2 - 2047 &= 162 \\
48^2 - 2047 &= 257 \\
49^2 - 2047 &= 354 \\
50^2 - 2047 &= 453 \\
51^2 - 2047 &= 554 \\
52^2 - 2047 &= 657 \\
53^2 - 2047 &= 762 \\
54^2 - 2047 &= 869 \\
55^2 - 2047 &= 978 \\
56^2 - 2047 &= 1089 = 33^2 \\
56^2 - 33^2 &= 2047 \\
(56 + 33) * (56 - 33) &= 2047 \\
89 * 23 &= 2047
\end{aligned}$$

1.12 *If $2^n + 1$ is prime, show that n is a power of 2. Is the converse true? (Davenport-Guy)*

Suppose - if possible - that $2^n + 1$ is prime, and $n = q * r$, where q is an odd prime divisor of n.

Then

$$2^{qr} + 1 = (2^r + 1)(1 - 2^r + 2^{2r} - \ldots + 2^{(q-1)r}).$$

Verification

$$(2^r * 1 - 2^r * 2^r + 2^r * 2^{2r} - \ldots + 2^r * 2^{(q-1)r}) + (1 - 2^r + 2^{2r} - \ldots + 2^{(q-1)r}) =$$

$$(2^r - 2^{2r} + 2^{2r+1} - \ldots - 2^{(q-1)r} + 2^{qr}) + (1 - 2^r + 2^{2r} - \ldots + 2^{(q-1)r}) =$$

$$1 + (2^r - 2^r) - (2^{2r} - 2^{2r}) + \ldots - (2^{(q-1)r} - 2^{(q-1)r}) + 2^{qr} =$$

$$1 + 2^{qr},$$

which shows that $(2^r + 1)|2^{qr} + 1$. Contradiction, $2^n + 1$ is prime. Therefore n does not have an odd prime divisor, so $n = 2^a, \quad a = 1, 2, \ldots$ Converse is false.

Let

$$F_n = 2^{2^n} + 1,$$

a Fermat number. We note that

$$F_m = F_0 F_1 \ldots F_{m-1} + 2$$

so every Fermat number is prime to every other Fermat number. However not every Fermat number is prime:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537 = 641 \times 6700417.$$

Proof of recursion:

$$\begin{aligned}
F_0 F_1 F_2 &= (2^{2^0} + 1)(2^{2^1} + 1)(2^{2^2} + 1) \\
&= (2^3 + 2^2 + 2 + 1)(2^{2^2} + 1) \\
&= (2^{2^2} - 1)(2^{2^2} + 1) \\
&= 2^{2^3} - 1 = F_3 - 2 \\
F_3 &= F_0 F_1 F_2 + 2
\end{aligned}$$

and so on for F_m.

1.13 *If P_1, P_2, are even perfect numbers with $6 < P_1 < P_2$ show that $P_2 > 16P_1$. (Davenport-Guy)*

Proof: First, we characterize even perfect numbers, by theorems due to Euler. Let n be a positive integer and let $\sigma(n)$ denote the sum of the divisors of n. By the Fundamental Theorem of Arithmetic any natural number (positive integer) can be represented in one and only one way as a product of primes. Thus $n = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$ with primes $p_1, p_2 \ldots p_s$ and positive integers $a_1, a_2 \ldots a_s$. First, we show

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \frac{p_2^{a_2+1} - 1}{p_2 - 1} \ldots \frac{p_s^{a_s+1} - 1}{p_s - 1}.$$

All divisors of n are of the form

$$p_1^{x_1} p_2^{x_2} \dots p_s^{x_s}$$

where

$$0 \le x_1 \le a_1,\ 0 \le x_2 \le a_2, \dots\ 0 \le x_s \le a_s.$$

Moreover, the summation of the finite geometric series is

$$p_1^0 + p_1^1 + p_1^2 \dots p_1^{a_1} = \frac{p_1^{a_1+1} - 1}{p_1 - 1}.$$

Therefore

$$\begin{aligned} \sigma(n) &= \sum_{x_1=0}^{x_1=a_1} \sum_{x_2=0}^{x_2=a_2} \dots \sum_{x_s=0}^{x_s=a_s} p_1^{x_1} p_2^{x_2} \dots p_s^{x_s} \\ &= \sum_{x_1=0}^{x_1=a_1} p_1^{x_1} \sum_{x_2=0}^{x_2=a_2} p_2^{x_2} \dots \sum_{x_s=0}^{x_s=a_s} p_s^{x_s} \\ &= \frac{p_1^{a_1+1} - 1}{p_1 - 1} \frac{p_2^{a_2+1} - 1}{p_2 - 1} \dots \frac{p_s^{a_s+1} - 1}{p_s - 1}. \end{aligned}$$

It also follows for numbers m and n, $(m, n) = 1$ that

$$\sigma(mn) = \sigma(m)\sigma(n)$$

and $\sigma(n)$ is a multiplicative (arithmethical) function. Let $p = 2^n - 1$ be a prime. Then

$$\frac{1}{2} p(p+1) = 2^{n-1}(2^n - 1)$$

is perfect. It is an even perfect number. Note that $p + 1 = 2^n$, hence $\frac{1}{2}(p+1) = 2^{n-1}$ and the sum of divisors of the latter number is

$$\sigma(\frac{1}{2}(p+1)) = 1 + 2 + \dots + 2^{n-1} = 2^n - 1.$$

This shows that a power of 2 is not a perfect number. Furthermore,

$$\sigma(p) = p + 1,$$

since $\sigma(n)$ is a multiplicative function and $(p, 2^{n-1}) = 1$,

$$\sigma(\frac{1}{2} p(p+1)) = \sigma(p)\sigma(\frac{1}{2}(p+1)).$$

$$\begin{aligned}
\sigma(\frac{1}{2}p(p+1)) &= \frac{2^n-1}{2-1}\frac{p^2-1}{p-1} \\
&= (2^n-1)(p+1) \\
&= p(p+1).
\end{aligned}$$

This shows that $\frac{1}{2}p(p+1)$ is perfect.

Moreover, every even perfect numbers is of this form. To see this let a be an even perfect number

$$a = 2^{n-1}u,\ \ u > 1, (2, u) = 1.$$

We have shown above that a a is not a power of 2. Therefore u is equal to a prime or a product of primes all greater than 2. By construction

$$2^n u = 2a,$$

and a is a perfect number

$$2a = \sigma(a).$$

$$\sigma(a) = \sigma(2^{n-1}u) = \sigma(2^{n-1})\sigma(u) = \frac{2^n-1}{2-1}\sigma(u)$$

Connecting the equations gives

$$2^n u = \frac{2^n-1}{2-1}\sigma(u),$$

by the definition of perfect number.

$$\sigma(u) = \frac{2^n u}{2^n-1}$$

$$\frac{2^n u}{2^n-1} = \frac{2^n u + u - u}{2^n-1} = \frac{(2^n u - u) + u}{2^n-1} = u + \frac{u}{2^n-1}$$

Therefore

$$\sigma(u) = u + \frac{u}{2^n-1}.$$

The left hand side is an integer, u is an integer so the second term on the right hand is an integer. Therefore $2^n - 1$ divides u

Thus $\sigma(u)$ is the sum of all positive divisors of u,there can only be two divisors, one is u the other is $\frac{u}{2^n-1}$. But 1 is certainly a divisor of u, therefore

$$\frac{u}{2^n-1} = 1$$

$$u = 2^n - 1$$

and $2^n - 1$ has no other positive divisor and $u = 2^n - 1$ is an odd prime. Let us collect our results. Every even perfect number has the form of

$$2^{p-1}(2^p - 1)$$

where p is a prime and $M_p = 2^p - 1$ is a Mersenne prime (see Exercise 1.11.)

If M_p and M_q are two consecutive Mersenne primes $2 < p \leq p + 2 \leq q$ then

$$\frac{2^{q-1}(2^q-1)}{2^{p-1}(2^p-1)} \geq \frac{2^{p+1}(2^{p+2}-1)}{2^{p-1}(2^p-1)} = 16\left(\frac{2^p - 2^{-2}}{2^p-1}\right) > 16$$

because

$$\left(\frac{2^p - 2^{-2}}{2^p-1}\right) > 1.$$

Bonus: *Every even perfect numbers ends with* 6 *or* 8*. (Shanks)*

Proof: If n is an even perfect number,

$$n = 2^{p-1}(2^p - 1)$$

with p prime. Every odd prime has the form $4m + 1$ or $4m + 3$. Write $p = 4m + 1,\ \ m \geq 1$

$$n = 2^{4m}(2^{4m+1} - 1) = 16^m(2 * 16^m - 1)$$

By induction, 16^m always ends in 6. Therefore $2 * 16^m - 1$ always ends in 1, and n in 6.

Similarly, if $p = 4m + 1\ \ m \geq 1$

$$n = 4 * 16^m(8 * 16^m - 1)$$

and $4 * 16^m$ ends in 4, while $8 * 16^m - 1$ ends in 7. Thus n ends in 8.

Finally, $p = 2$ gives $n = 6$.

1.14 If p, q are odd primes, show that $p^a q^b$ can not be perfect.
Proof: The number n is *perfect* if the sum of its divisors, including 1, but excluding n, is equal to n itself.

$$\begin{aligned} n &= p^a q^b \\ \sigma(n) &= 2n \\ \sigma(n) &= \left(1 + p + p^2 + \ldots + p^a\right)\left(1 + q + q^2 + \ldots + q^b\right) \end{aligned}$$

Suppose - if possible - that

$$\begin{aligned} \sigma(p^a q^b) &= 2p^a q^b \\ \frac{p^{a+1} - 1}{p - 1}\frac{q^{b+1} - 1}{q - 1} &= 2p^a q^b \\ \frac{p^{a+1} - 1}{p^a}\frac{q^{b+1} - 1}{q^b} &= 2(p-1)(q-1) \\ \left(p - \frac{1}{p^a}\right)\left(q - \frac{1}{q^b}\right) &= 2(p-1)(q-1) \\ \left(p - \frac{1}{p^a}\right) &< p \\ \left(q - \frac{1}{q^b}\right) &< q \\ \left(p - \frac{1}{p^a}\right)\left(q - \frac{1}{q^b}\right) &< pq \\ \frac{p}{(p-1)}\frac{q}{(q-1)} &> 2. \end{aligned}$$

Look at the first two odd primes $p = 3, q = 5$

$$\frac{3}{2} \times \frac{5}{4} = \frac{15}{8} < 2.$$

Notice further that all odd primes are a subset of the odd numbers $2n+1 > 1$, $n = 1, 2, 3, \ldots$ and the sequence

$$\frac{3}{2} > \frac{5}{4} > \ldots > \frac{2n+1}{2n}$$

is strictly monotone decreasing. Let r, s be two odd primes $r < s$. Then

$$\frac{r}{(r-1)}\frac{s}{(s-1)} \leq \frac{3}{2} \times \frac{5}{4} = \frac{15}{8} < 2.$$

Therefore

$$\frac{p}{(p-1)}\frac{q}{(q-1)} < 2$$

for odd primes p, q. Contradiction, hence $p^a q^b$ cannot be perfect.

(Elementary, my dear Watson .)

12.5 Tutorial 4.

- Higher Arithmetic
- *Spartan Old School*
- Last revision March 29, 2016

Exercises

6. Examples of *prime factorization* :
i) N=999

$$\begin{aligned} 999 : 3 &= 333 \\ 333 : 3 &= 111 \\ 111 : 3 &= 37 \\ 37 &= 37 \end{aligned}$$

$N = 3 * 3 * 3 * 37.$

ii) N=1001, by *Fermat's method* .

$31^2 < 1001 < 32^2$

Searching for a complete square:

$$\begin{aligned} 32^2 - N &= 23 \\ 33^2 - N &= 88 \\ 34^2 - N &= 155 \\ 35^2 - N &= 224 \\ 36^2 - N &= 295 \\ 37^2 - N &= 368 \\ \ldots &= \ldots \\ 45^2 - N &= 1024 = 32^2 \\ 45^2 - 32^2 &= N.\surd \end{aligned}$$

$N = (45 + 32)(45 - 32) = 77 * 13 = 7 * 11 * 13.$

iii) N=1729, by *Fermat's method* .

$$41^2 < 1729 < 42^2$$

$$\begin{aligned} 42^2 - N &= 35 \\ \dots &= \dots \\ 55^2 - N &= 1296 = 36^2 \\ 55^2 - 36^2 &= N.\surd \end{aligned}$$

$$N = (55 + 36)(55 - 36) = 91 * 19 = 7 * 13 * 19.$$

iv) N=11111 The smallest prime factor in N (if any) is not greater than $\sqrt{N}$. Thus we consider the primes up to $\sqrt{N} < 106$:

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97
101	103	107	...	...
...	...	...	...	...
...	...	271	...	...

The first prime that divides N is 41.

$$11111 : 41 = 271$$

It turns out that 271 is also a prime, therefore

$$N = 41 * 271.$$

7. Examples of *Euclidean algorithm* : Find the *highest common factor* of

$i)$ $6188, 4709$ $ii)$ $81719, 52003, 33649, 30107.$

Proof: i)

$$\begin{aligned} 6188 &= 1 * 4709 + 1479 \\ 4709 &= 3 * 14709 + 272 \\ 1479 &= 5 * 272 + 119 \\ 272 &= 2 * 119 + 34 \\ 119 &= 3 * 34 + 17 \\ 34 &= 2 * 17 + 0 \end{aligned}$$

The highest common factor of 6188, 4709 is 17, the last positive remainder. Next, express the h.c.f as a linear (Diophantine) combination of $a = 6188$ and $b = 4709$.

$$\begin{aligned} 1479 &= a - b \\ b &= 3 * (a - b) + 272 \\ 272 &= 4b - 3a \\ 119 &= 16a - 21b \\ 34 &= 46b - 35a \\ 17 &= 121a - 159b. \end{aligned}$$

Check:

$$121a - 159b = 121 * 6188 - 159 * 4709 = 748748 - 748731 = 17.\surd$$

ii)

$$m(a_1, a_2) = m_2; m(m_2, a_3) = m_3; m(m_3, a_4) = m_4$$

$$\begin{aligned} 81719 &= 1 * 52003 + 29716 \\ 52003 &= 1 * 29716 + 22287 \\ 29287 &= 1 * 22287 + 7429 \\ 22287 &= 3 * 7429 \end{aligned}$$

$$\begin{aligned} 81719 : 7429 &= 11 \\ 52003 : 7429 &= 7 \\ m_2 &= 7429. \end{aligned}$$

$$
\begin{aligned}
33649 &= 4 * 7429 + 3933 \\
7429 &= 1 * 3933 + 3496 \\
3933 &= 1 * 3496 + 437 \\
3496 &= 8 * 437
\end{aligned}
$$

$$
\begin{aligned}
81719 : 437 &= 187 \\
52003 : 437 &= 119 \\
33649 : 437 &= 77 \\
m_3 &= 437.
\end{aligned}
$$

$$
\begin{aligned}
30107 &= 68 * 437 + 391 \\
437 &= 1 * 391 + 46 \\
391 &= 8 * 46 + 23 \\
46 &= 2 * 23.
\end{aligned}
$$

$$m_4 = 23.$$

8. Show that

$$n(n+1)(2n+1)$$

is divisible by 6.

Proof : Write $N = n(n+1)(2n+1)$. If n is odd then $n+1$ is even and N is divisible by 2. If n is even then N is divisible by 2.

If $n \equiv 0$ $(mod 3)$ then N is divisible by 3. If $n \equiv 1$ $(mod 3)$ then $2n+1 \equiv 0$ $(mod 3)$ and N is divisible by 3. If $n \equiv 2$ then $n+1 \equiv 0$ $(mod 3)$ and N is divisible by 3. Since n is in exactly one of the above equivalence classes N is divisible by 3.

Therefore N is divisible by both 2 and 3, thus by 6.

9. Show that

$$m + \frac{1}{2}(m+n-1)(m+n-2)$$

runs through the whole set of positive integers without repetition as m and n run through the set of all positive integers.

Discussion: Consider the lattice points (points with integer coordinates) in the positive quadrant of the Cartesian coordinate system. As m and n run through the whole set of positive integers the ordered pair (m, n) runs through the lattice points :

$$A = \{(m, n),\ m = 1, 2, \ldots;\ n = 1, 2, \ldots\}.$$

Write

$$f(m, n) = m + \frac{1}{2}(m + n - 1)(m + n - 2).$$

The *range* of this function is A since (m, n) takes on every possible pair of positive integers. Further, f is an integer because exactly one of the two consecutive numbers $(m + n - 1)$,$(m + n - 2)$ is even. So the *image* of f is a subset of the set of positive integers. We will show that this map is in fact, bijective: it maps the lattice points of the positive quadrant onto the set of positive integers. First, we shall consider a subset of A. Take

$$A_6 = \{(m, n),\ m = 1, 2, \ldots, 5;\ n = 1, 2, \ldots, 5;\ m + n \leq 6\}.$$

The points belonging to A_6 are on the lower left corner of A. A_6 has a triangular shape, there are 15 points in it, and A_6 can be covered by

$$\begin{aligned}
D_1 &= \{(1, 1)\} \\
D_2 &= \{(1, 2), (2, 1)\} \\
D_3 &= \{(1, 3), (2, 2), (3, 1)\} \\
D_4 &= \{(1, 4), (2, 3), (3, 2), (4, 1)\} \\
D_5 &= \{(1, 5), (2, 4), (3, 3), (4, 2), (5, 1)\}.
\end{aligned}$$

The sets $D_1, D_2, \ldots, D_5$ provide a *cover* of A_6:

$$D_1 \cup D_2 \cup, \ldots \cup D_5 = A_6;\ D_1 \cap D_2 \cap, \ldots \cap D_5 = \emptyset.$$

Notice also that $D_1, D_2, \ldots, D_5$ look like "slanting diagonals" on latice points. Another interesting feature is that

$$\frac{1}{2}(m + n - 1)(m + n - 2) = const$$

on each D_i. Let us calculate $f(m,n)$ on A_6 :

$$f(1,1) = 1 + \frac{1}{2}(1+1-1)(1+1-2) = 1,$$

$$f(1,2) = 1 + \frac{1}{2}(1+2-1)(1+2-2) = 2,$$

$$f(2,1) = 2 + \frac{1}{2}(2+1-1)(2+1-2) = 3,$$

$$D_3 : \ f(1,3) = 4, \ f(2,2) = 5, \ f(3,1) = 6,$$

$$D_4 : \ f(1,4) = 7, \ f(2,3) = 8, \ f(3,2) = 9, f(4,1) = 10,$$

the pattern is discernible,

$$D_5 : \ f(1,5) = 11, \ f(2,4) = 12, \ f(3,3) = 13; f(4,2) = 14, \ f(5,1) = 15.$$

Define

$$\begin{aligned} C_1 &= \{1\} \\ C_2 &= \{2,3\} \\ C_3 &= \{4,5,6\} \\ C_4 &= \{7,8,9,10\} \\ C_5 &= \{11,12,13,14,15\}. \end{aligned}$$

Note that the sets $C_1, C_2, \ldots, C_5$ provide a *cover* of $\{1,2,3,\ldots,15\}$, moreover, each C_i is an ordered set of positive integers; the minimal element of each C_k is the sum of the first $k-1$ positive integers plus 1, the maximal element of each C_k is the sum of the first k positive integers, $i > 1$. So having partitioned A and $\{1,2,3,\ldots,15\}$ we note that f maps each D_i onto C_i, $i = 1,2\ldots5$. Therefore f is a *bijection* , and f^{-1} induces a linear order on A_6.

Proof: Extend the above construction by adjoining successive "slanting diagonals". Then each positive number will be associated with exactly one ordered pair of positive integers, (m,n).

12.6 Tutorial 5.

Summary

- Geometry
- *Hajós - Strohmayer*
- Last revision March 29, 2016

Triangle Inequalities 3.2

Notation: Standard. $\triangle ABC$ has vertices A, B, and C ; sides AB, BC and CA, and angles α, β, γ. Vertices A, B, and C are in counterclockwise direction, the sides opposite to A, B, and C are denoted by a, b, and c, respectively. Angle α is at A; β at B; and γ at C. The angle at A can be marked as $\angle A$.

A *cevian* of a triangle is a line from a vertex to a point on the opposite side, or its extension.(Giovanni Ceva, geometer, Italy, 17th century). An angle *bisector* of a triangle is a line that bisects an angle and extends to the opposite side. A *median* of a triangle is a line from a vertex to the midpoint of the opposite side. An *altitude* of a triangle is a line from a vertex perpendicular to the opposite side. Bisectors, medians, altitudes are cevians.

The triangle inequality says that any side is less than the sum of the other two sides.

9. Any side of a triangle ABC is less than half the perimeter.

Proof:

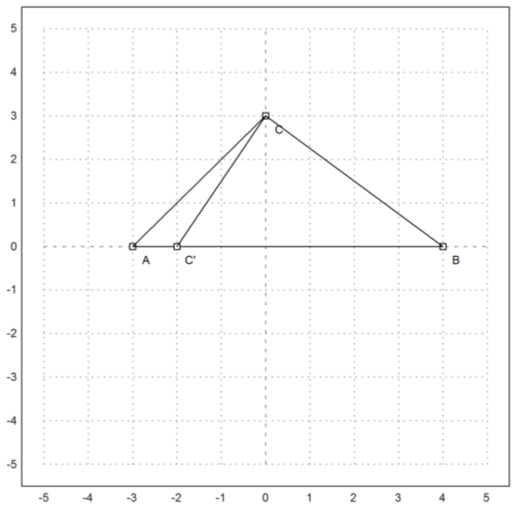
$$a < b + c;\ b < a + c;\ c < a + b;$$

$$a + a < b + c + a;\ b + b < a + c + b;\ c + c < a + b + c;$$

$$a < \frac{a + b + c}{2};\ b < \frac{a + b + c}{2};\ c < \frac{a + b + c}{2};$$

10. Given $\triangle ABC$. Let C' be a point on AB. Then

$$\frac{1}{2}(AC + BC - AB) < CC' < \frac{1}{2}(AC + BC + AB)$$



Proof: Case 1.

Let C' be an inner point of AB.

$$AC + AC' > CC'$$

$$CB + C'B > CC'$$

$$AC + CB + (AC' + C'B) > 2CC'$$

$$CC' < \frac{AC + CB + AB}{2} = \frac{1}{2}(AC + BC + AB).$$

This proves the right-hand side. Moreover

$$AC < AC' + CC'$$

$$BC < C'B + CC'$$

$$AC + BC < AB + 2CC'$$

$$AC + BC - AB < 2CC'$$

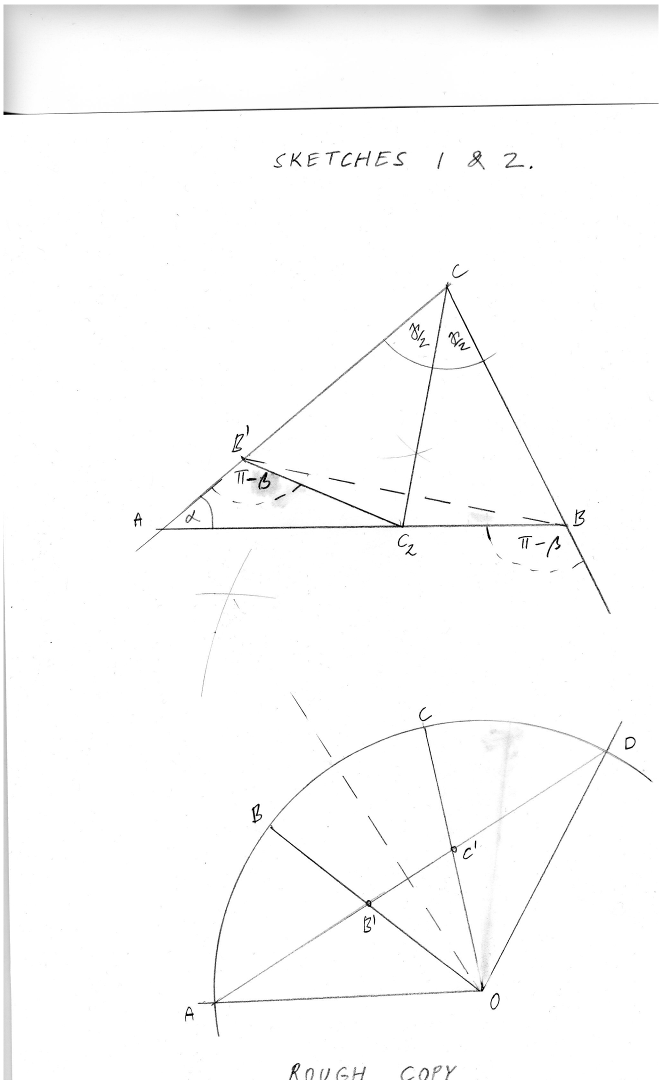
$$\frac{AC + BC - AB}{2} < CC'$$

This proves the left-hand side. Case 2. Now suppose C' is an end point, say $C' = A$

$$CC' = CA = AC < \frac{1}{2}(AC + BC + AB)$$

any side is less than half the perimeter. This proves the right-hand side of the inequality. As for the left-hand side, we have - trivially -

$$\begin{aligned} AC &\leq AC \\ BC &\leq AB + AC \\ AC + BC &\leq AB + 2AC \\ AC + BC - AB &\leq 2AC \\ \frac{1}{2}(AC + BC - AB) &\leq AC. \end{aligned}$$


SKETCHES 1 & 2.
C
γ/2
γ/2
B'
π-β
A
α
C2
B
π-β
C
D
B
C'
B'
A
O
ROUGH COPY

12.7 Tutorial 6.

Summary

- Higher Arithmetic
- *Spartan Old School*
- Last revision March 29, 2016

"Hard Time" Primes

Exercise 162: *In the 4000 numbers*

$$f(n) = n^6 + 1091,\ n = 1, 2, \ldots 4000,$$

there is only one prime. Find it. (Shanks)

Discussion: We claim that

$$f(3906) = 3906^6 + 1091$$

is the only prime in $n = 1, 2, \ldots 4000$. We cannot verify our claim by direct calculation on our current desktop computer due to limitation on the largest representable integer, $f(3906) \approx 3.5 \times 10^{21}$. Therefore we shall find our number by modular arithmetic based on the following observation:

Let p be a prime, then

$$n \equiv n' \pmod{p} \Rightarrow f(n) \equiv f(n') \pmod{p}.$$

This suggests a simple algorithm. Write

$$q \equiv 1091 \pmod{p},$$

and let a run through the complete residue system modulo p,

$$0,\ 1,\ 2,\ \ldots\ p-1.$$

Calulate a^6:

$$0^6,\ 1^6,\ 2^6,\ \ldots\ (p-1)^6$$

modulo p. Check

$$f(a) = a^6 + q, \quad a = 0, 1, 2, \ldots p-1, (\text{mod } p)$$

If

$$f(a) \equiv 0 \pmod{p}$$

then exclude a, and with it all numbers between 1 and 4000 that belong to the residue class represented by a, from further consideration.

We shall take the first 25 primes

$$2, 3, 5, \ldots 89, 97$$

and screen the numbers $n = 1, 2, \ldots 4000$. This is a numerical experiment, we expect to reduce the number of possible primes.

Take $p = 2$.

$$1091 \equiv 1, \quad (\text{mod } 2)$$

$$n \equiv 1 \pmod{2}$$

then

$$f(n) \equiv 0 \pmod{2}.$$

Therefore $f(n)$ is a composite number for odd n. Hence the odd numbers are exluded.

Next, $p = 3$.

$$1091 \equiv 2, \quad (\text{mod } 3)$$

so if

$$n^6 \equiv 1, \quad (\text{mod } 3)$$

then $f(n)$ is composite:

$$f(n) = n^6 + 1091 \equiv 1 + 2 \equiv 0, \quad (\text{mod } 3).$$

Therefore $n \equiv \pm 1, \quad (\text{mod } 3)$ excluded. For example

$$n = 4, n \equiv 1 \pmod{3}$$

$f(4) = 4^6 + 1091 = 5181 = 1729 * 3$

$f(4) \equiv 0 \pmod 3$

$n = 5, n \equiv -1 \pmod 3$

$f(5) = 5^6 + 1091 = 16716 = 5572 * 3$

$f(5) \equiv 0 \pmod 3$.

Next prime is $p = 5$. Let us examine

$0, 1, 2, 3, 4$

the complete residue system of modulo 5,

$0^6 = 0,\ 1^6 = 1,\ 2^6 = 64,\ 3^6 = 729,\ 4^6 = 4096$

$0^6 \equiv 0,\ 1^6 \equiv 1,\ 2^6 \equiv 4,\ 3^6 \equiv 4,\ 4^6 \equiv 1,\ \pmod 5$

Since $1091 \equiv 1,\ \pmod 5$

$f(n) = n^6 + 1091 \equiv 0, \quad \pmod 5$

if and only if $n \equiv 2 \pmod 5$ or $n \equiv 3 \pmod 5$. Thus such n-s are excluded.

For the next prime, $p = 7$ let us recall *Fermat's Theorem*

$a^{p-1} \equiv 1,\ \pmod p\ (a, p) = 1$

Since

$(1091, 7) = 1,\ 1091 \equiv 6, \pmod 7$

$a^6 + 1091 \equiv 0 \pmod 7,\ a = 1, 2, 3, 4, 5, 6.$

Therefore all residue classes $a = 1, 2, 3, 4, 5, 6, \pmod 7$ are rejected.

We continue in this manner and *screen* the the range of n using the remaining small primes. The examinaton of the residue classes may yield zero, one, or more than one solutions. We shall not enter into finer analysis, just list the suitable residue classes.

```
program fermat_0
    ! n^6+1091 .eqv. 0 (mod p) , n=1,2, ...4000; small primes p= 2,3, ... 67, 71
implicit none
integer, dimension (25) :: small
integer, dimension (60,4) :: array
integer i,j,k,l,m, n, p, pm1, q , n6
integer istop, nbig, ierror
parameter(nbig=1091)
! list of small primes
small(1)=2
small(2)=3
small(3)=5
small(4)=7
small(5)=11
small(6)=13
small(7)=17
small(8)=19
small(9)=23
small(10)=29
small(11)=31
small(12)=37
small(13)=41
small(14)=43
small(15)=47
small(16)=53
small(17)=59
small(18)=61
small(19)=67
small(20)=71
small(21)=73
small(22)=79
small(23)=83
small(24)=89
small(25)=97
!
array=0
!input
k=0
```

```
loop_2000: do j=1,25
    p=small(j)
    pm1=p-1
    q=mod(nbig,p)
loop_1000: do i= 0,pm1
    n6=i*i*i*i*i*i
    if( mod(n6,p) + q == p ) then
        k=k+1
        array(k,1)=i
        array(k,2)= mod(n6,p)
        array(k,3)= q
        array(k,4)= p
        print*, array(k,1),array(k,2),array(k,3),array(k,4)
        endif
    end do loop_1000
  end do loop_2000
   ! next, print to file
open(unit=10,file="Shanks0.dat",status="old",action="write",iostat=ierror)

if(ierror/=0) then
print*, "failed to open Shanks0.dat"
stop
else
print*, "  ***   opened Shanks0.dat"
end if
write(10,100) k
100 format('Shanks0 data:', i7)

do i=1,k
write(10,101) array(i,1),array(i,2),array(i,3),array(i,4)
101 format (4(3x,i8))
end do
close(unit=10)
print*, "  ***   closed Shanks0.dat"


end program
```

The output is table Shanks0.dat. As discernable from the code, the first column from right contains prime p, the second column from the right contains is $q \equiv 1091 \pmod{p}$, the next is $mod(a^6, p)$, and finally a.

```
Shanks0 data:     33
           1           1           1           2
           1           1           2           3
           2           1           2           3
           2           4           1           5
           3           4           1           5
           1           1           6           7
           2           1           6           7
           3           1           6           7
           4           1           6           7
           5           1           6           7
           6           1           6           7
           2           9           2          11
           9           9           2          11
           1           1          12          13
           3           1          12          13
           4           1          12          13
           9           1          12          13
          10           1          12          13
          12           1          12          13
           4          11           8          19
           6          11           8          19
           9          11           8          19
          10          11           8          19
          13          11           8          19
          15          11           8          19
           8          13          10          23
          15          13          10          23
          16          16          25          41
          25          16          25          41
          11          37          10          47
          41          37          10          47
          41          30          29          59
          30          45          26          71
```

The next program screens $n = 1, 2, 3, \ldots 4000$, and rejects the numbers that fall into any of the residue classes identified in *Shanks0.dat*.

```
program fermat_2
!screen n=1,2, ... 4000 for f(n)=n^6+1091
implicit integer (i-n)
integer, dimension (1:1024) :: array
real x0,y
parameter(nbig=4000)
!
array=0
!
j=0
do i= 1,4000
    if(mod(i,2)==1) cycle
    if(mod(i,3)==1.or.mod(i,3)==2) cycle
    if(mod(i,7)/=0) cycle
    if(mod(i,5)==2) cycle
    if(mod(i,5)==3) cycle
    if(mod(i,11)==2) cycle
    if(mod(i,11)==9) cycle
    if(mod(i,13)==1) cycle
    if(mod(i,13)==3) cycle
    if(mod(i,13)==4) cycle
    if(mod(i,13)==9) cycle
    if(mod(i,13)==10) cycle
    if(mod(i,13)==12) cycle
    if(mod(i,19)==4) cycle
    if(mod(i,19)==6) cycle
    if(mod(i,19)==9) cycle
    if(mod(i,19)==10) cycle
    if(mod(i,19)==13) cycle
    if(mod(i,19)==15) cycle
    if(mod(i,23)==8) cycle
    if(mod(i,23)==15) cycle
    if(mod(i,41)==16) cycle
    if(mod(i,41)==25) cycle
    if(mod(i,47)==11) cycle
```

```
    if(mod(i,47)==36) cycle
    if(mod(i,71)==30) cycle
    if(mod(i,71)==41) cycle
    j=j+1
    array(j)=i
end do

   ! next, print to file
open(unit=10,file="Shanks1.dat",status="old",action="write",iostat=ierror)

if(ierror/=0) then
print*, "failed to open Shanks1.dat"
stop
else
print*, "  ***   opened Shanks1.dat"
end if
write(10,100) j
100 format('Shanks1 data:', i7)
do i=1,100,5
write(10,101) array(i),array(i+1),array(i+2),array(i+3),array(i+4)
101 format (5(3x,i7))
end do
close(unit=10)
print*, "  ***   closed Shanks1.dat"
end program
```

The result is a list of 14 numbers:

```
Shanks1 data:     14
       210        546        630       1176       1386
      1974       2184       2520       2646       2940
      3024       3360       3570       3906          0
```

This is a significant reduction, now we have only 14 prime cadidates. Finally, we test these numbers by *trial division* based on this program:

```
PROGRAM  Factorize
    ! Dr C-K Shene, Michigan Techn. Univ.
   IMPLICIT  NONE
```

```
   INTEGER(kind=selected_int_kind(15)) :: Input
   INTEGER(kind=selected_int_kind(15))  :: Divisor
   INTEGER(kind=selected_int_kind(15))  :: Count

  ! WRITE(*,*)  'This program factorizes any integer >= 2 --> '
    !READ(*,*)   Input

!Input=20**6+1091=64001091=
   Input=9261000+1091

   Count = 0
   DO                          ! here, we try to remove all factors of 2
      IF (MOD(Input,2) /= 0 .OR. Input == 1)  EXIT
      Count = Count + 1        ! increase count
      WRITE(*,*)  'Factor # ', Count, ': ', 2
      Input = Input / 2        ! remove this factor from Input
   END DO

   Divisor = 3                 ! now we only worry about odd factors
   DO                          ! 3, 5, 7, .... will be tried
      IF (Divisor > Input) EXIT    ! if a factor is too large, exit and done
      DO                       ! try this factor repeatedly
         IF (MOD(Input,Divisor) /= 0 .OR. Input == 1)  EXIT
         Count = Count + 1
         WRITE(*,*)  'Factor # ', Count, ': ', Divisor
         Input = Input / Divisor   ! remove this factor from Input
      END DO
      Divisor = Divisor + 2    ! move to next odd number
   END DO

END PROGRAM  Factorize
```

Only trivial modifications are needed

```
program fermat_4
! f(n)=n^6+1091
implicit none
integer(kind=selected_int_kind(15))::n,q,i,i2,i4,i6
```

```
integer(kind=selected_int_kind(15))::nbig,qbig,odd
integer(kind=selected_int_kind(15)):: marker1, marker2, marker3
WRITE(*,*)  'This program factorizes f(n), n<4001 --> '
READ(*,*)   n
if(n>4001) then
print*, " n is too big ", n
stop
endif
!
qbig=1091
nbig=n*n*n+qbig
print*, " nbig=", nbig
print*, " n=", n
odd=-1
marker1=nbig/4
marker2= marker1+marker1
marker3= marker2+marker1
!
do i= 3,nbig,2
    ! can run faster if 6k+1,6k-1.eqv.6k+5 are used ?
    ! markers
    if(i==marker1) print*, " i=", i
    if(i==marker1+1) print*, " i=", i
    if(i==marker2) print*, " i=", i
    if(i==marker2+1) print*, " i=", i
    if(i==marker3) print*, " i=", i
    if(i==marker3+1) print*, " i=", i
    ! keeping numbers low
    i2= mod(n,i)*mod(n,i)
    i2=mod(i2,i)
    i4= i2*i2
    i4=mod(i4,i)
    i6= i4*i2
    i6= mod(i6,i)
    q = mod(qbig,i)
    ! check
    if(mod(i6+q,i)/=0) cycle
    print*, " i=", i
```

```
    print*, "i2=", i2
    print*, "i4=", i4
    print*, "i6=", i6
    print*, " q=",  q
    print*, "f(n) is divisible by"
    odd=i
    exit
end do
! -1 means prime
 print*, " div =", odd

end program
```

divisor	$f(n)$
109	$f(210)$
2129	$f(546)$
347	$f(630)$
34996691	$f(1176)$
6282607	$f(1386)$
68891	$f(1974)$
199	$f(2184)$
199	$f(2520)$
383	$f(2646)$
13163	$f(2940)$
4153	$f(3024)$
233	$f(3360)$
19379	$f(3570)$
-1	$f(3906)$

12.8 Miscellaneous Notes

12.8.1 Current interests

Spartan Old School Tutorial: Calculus, Algebra and Number Theory, Geometry; with basic programming, Latex typesetting.

Classics in Pure Math: Pólya - Szegő: Aufgaben und Lehrsätze aus der Analysis,

Classics in Applied Math

Mathematical Modelling

12.8.2 Envoy

Jánoshalmi Spartacus Sport Egylet
A Verhetetlen Tizenegy:
Tirnauer (1) -
Ásó (2), Kapa (3) -
Steinetz (4), Dr Melvin No, Privatdozent(5), Podhola (6) -
Sipőcz (7), Kohn Geÿza (8), Halász (9), Vadász (10), Madarász (11) .