A Computer Motivated Study of Problems in Number Theory

Michael Blinov[1], Nurit Zehavi[2] and Sarah Black[3]

[1]Mathematics Department, The Weizmann Institute of Science, Rehovot, Israel

e-mail: blinov@wisdom.weizmann.ac.il

[2]Science Teaching Department, The Weizmann Institute of Science, Rehovot, Israel

e-mail: nurit.zehavi@weizmann.ac.il

[3]Mathematics Department, Michlalah-Jerusalem College, Jerusalem, Israel

e-mail: sblack1@macam.ac.il

A Computer Motivated Study of Problems in Number Theory

Abstract

Number Theory is a subject that fascinates both professional number-theorists and "recreational" mathematicians. The reason is clear: the objects that are studied are concrete, thus useful intuitions about them can be developed through experimenting with easy examples. Moreover, employing the computer in such investigations enables many more cases to be verified than can be done manually, thus facilitating the statement of a true conjecture, which subsequently requires a proof. Additionally, it sometimes paves the way towards other, related conjectures.

The aim of this paper is to report on such a scenario; namely, the presentation of a problem, its investigation using the computer and the subsequent problems which arose as a result. All of these explorations were interlaced with a study of the necessary number theoretic background to effectively tackle the evolving problems.

1. Introduction

The problems discussed in this paper originated from a graduate course, *Problem Solving, using Computer Algebra Systems (CAS)*, given for Israeli mathematics teachers by the second author at the Weizmann Institute of Science. (The first author was the teaching assistant in the course, and the third author adapted the materials for number theory classes.) The main goal of the course was to enable teachers to refresh and extend their

mathematical knowledge using CAS software as a mathematical tool and a programming language. We used *Derive*, but users of other programs can easily replicate the tasks. Since this was a new graduate course, the authors were engaged in producing computer-based activities to achieve the goal of the course. One activity in Number Theory, originally a simple computer exercise, developed into interesting theory, where each problem was followed by an answer, and each answer -- again by a problem. The computer played a significant role in that sequence of investigations, and as a result we were quickly led into the world of Number Theory, starting from classical concepts and leading eventually to a conjecture due to Artin in1927, which remains unproved!

Due to the logistic problem of simultaneously presenting the flow of ideas that evolved in the course and the related mathematical background, the paper is presented in the following format. For the convenience of the reader, the sequence of investigations will be described with intermittent references to a web document "Mathematical Appendix" (see http://stwww.weizmann.ac.il/g-math/mathcomp/number-theory.pdf) containing the relevant mathematical theory

2. Starting from 'simple' problems

We chose to introduce the software via problems in Number Theory for three reasons:

1. The numerical power offered by a CAS is very impressive and quite different from other technological tools.
2. Problems in Number Theory appear in the repertoire of mathematicians at all levels.

3. We can demonstrate clearly how the software's programming language constitutes the language of mathematics, using examples from Number Theory. For example, the *Derive* statement, "*DIMENSION(SELECT(PRIME(k), k, 1,100))*" in effect says "create a vector whose elements were *SELECTED* from the given sequence according to the primality criterion, and report the number of elements in this vector".

Problem 1. *Euclid proved that there is infinite number of primes. How many primes are between: 1 and 5,000? 1 and 10,000? 1 and 50,000? What can you say about the distribution of primes among the natural numbers?*

To get some feeling of the answers, the participants were advised to utilize the functions *PRIME, SELECT, DIMENSION,* and to represent the findings in a graph (Figure 1). Note that this graph is composed of 121 discrete points created by the *TABLE* command.

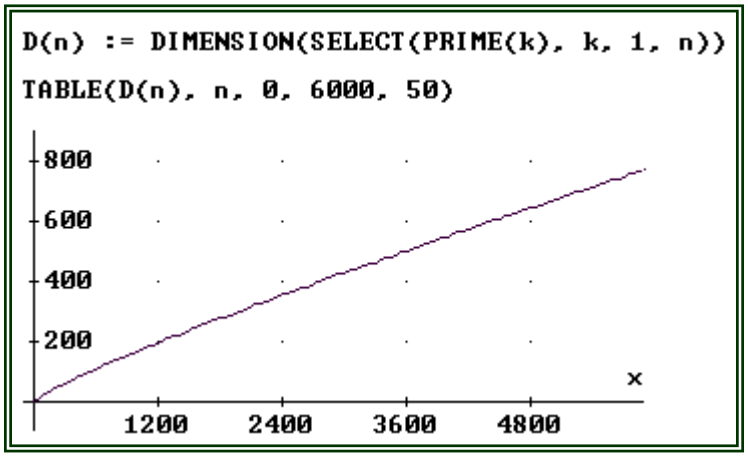

Figure 1: Distribution of prime numbers

Participants were then encouraged to surf to Web sites (see references) where they saw similar graphs to those they had produced and read about The Prime Number Theorem:

The number of primes not exceeding N, $\pi(N)$ *is asymptotic to* $\frac{N}{\ln N}$ *(notation:* $\pi(N) \sim \frac{N}{\ln N}$*).*

True mastery of this topic requires substantial mathematical knowledge in real analysis and thus was beyond the scope of the course. However, as a cornerstone of classical number theory, it was not an issue to be avoided. Hence, we came up with the following didactical bridge:

(a) Find the number of primes in the intervals $[10^m, 10^{m+1}-1]$ for different values of *m*, using the command *DIMENSION(SELECT(PRIME(n),n,*10^m*,* 10^{m+1}*-1));*

(b) Explain the results of (a) in the context of the Prime Number Theorem (PNT).

The intervals were chosen to draw the learner's attention to the connection between the exponents in the definition of the intervals, and the logarithmic function in the theorem. The increasingly closer connection between the findings and the results of the PNT, served to reinforce participants' understanding of the statement of the theorem (see Note 1, Mathematical Appendix.)

The object of the next investigation was to try and investigate empirically how many natural numbers x, in an interval determined by a given n, satisfied the property "x^2-1 is divisible by n ". Indeed ,for a fixed n, and a multiple tn of n for t an arbitrary positive integer, we are looking at all integers in the interval $\{tn, tn+1, tn+2, ...tn+n-1\}$ which is the interval between tn and $(t+1)n$. Specifically,

Problem 2. *Let* $n \geq 1$ *be a natural number. From amongst the numbers nt, nt+ 1, nt + 2,…, nt + (n - 1), find those x = nt + k for which* x^2 *- 1 is divisible by n. What is, in your opinion, the answer for general n?*

The problem seemed a simple programming exercise: For $n = 2$, we have $2t$, $2t+1$, of which only $(2t + 1)^2 - 1$ is divisible by two. For $n = 3$ it is readily seen that the expression $x^2 - 1$ divisible by 3 only for x of the forms $x = 3t + 1$ or $x = 3t + 2$. For $n = 4$, amongst $x = 4t$, $x = 4t + 1$, $x = 4t + 2$, and $x = 4t + 3$, $x^2 - 1$ is divisible by 4 only for $x = 4t + 1$ or $x = 4t + 3$. Note that it is enough to consider just k between 1 and $n-1$ instead of all natural numbers x, (see Note 2, Mathematical Appendix.). Thus, for larger values of n, we apply the command that prints all values of k between 1 and $n - 1$, such that the greatest common divisor of $k^2 - 1$ and n is equal to n. The results for $2 \le n \le 7$ are illustrated in Figure 2 below:

```
      SELECT(GCD(k^2 - 1, n) = n, k, 1, n - 1)
      ========================================

SELECT(GCD(k^2 - 1, 3) = 3, k, 1, 3 - 1) = [1, 2]
SELECT(GCD(k^2 - 1, 4) = 4, k, 1, 4 - 1) = [1, 3]
SELECT(GCD(k^2 - 1, 5) = 5, k, 1, 5 - 1) = [1, 4]
SELECT(GCD(k^2 - 1, 6) = 6, k, 1, 6 - 1) = [1, 5]
SELECT(GCD(k^2 - 1, 7) = 7, k, 1, 7 - 1) = [1, 6]
```

Figure 2: k satisfying GCD(k^2 –1, n) =n for n=3,4, …, 7

For $n=2, 3,...,7$ the computer investigation seemed to indicate that $x^2 - 1$ is divisible by n only for $x = nt + 1$ and $x = nt + (n - 1)$. However, the case $n = 8$ yielded 4 solutions: *SELECT(GCD(k^2 - 1, 8) = 8, k, 1, 7) = [1, 3, 5, 7]*. For subsequent values of n,

Figure 3 shows the list of k's, satisfying GCD(k^2 - 1, n) = n) for n between 8 and 24.

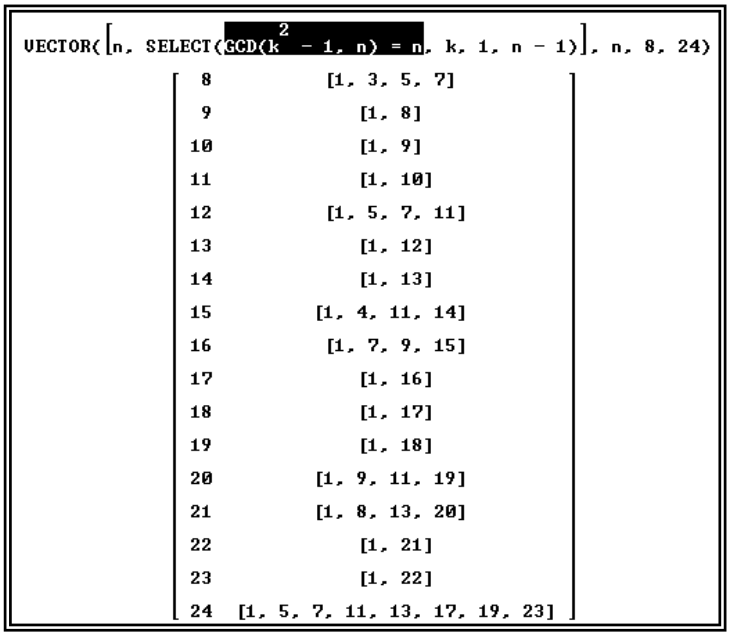

Figure 3: k satisfying GCD(k^2 – 1, n) =n for n = 8, 9, …, 24

Basically there are two issues of interest in the results shown in Figure 3:

(a) numerical patterns in the lists;

(b) the growth of the dimension of the lists; more specifically: if and for what values of *n*, lists of 12 or 16 numbers would be obtained.

To find an answer to these questions, we defined *F(n)* as the number of *k* values satisfying *GCD(k^2 - 1, n)=n*. Thus,

F(n):= DIMENSION(SELECT(GCD(k^2 - 1, n)=n, k, 1, n - 1)).

Whilst *F(24)=8*; for larger *n*'s, (up to *80…. 119*) the values of *F(n)* are all *2,4* or *8*. But At this point it was evident that the 'simple' problem needed further investigation. It was conjectured that the value of *F (n)* was intimately connected with the factorization of n.

Problem 3. *Find F(n).*

We sat down to work on the problem with *Derive*. Looking for patterns in the data by factorizing the *n*'s where a 'jump' occurred, yielded the following results:

n	*Factorisation of n*	*F(n)*
8	2^3	4
24	$2^3 \cdot 3$	8
120	$2^3 \cdot 3 \cdot 5$	16

The conjecture was that the next greater value of *F(n)* should be *32* and it should be achieved for $n = 2^3 \cdot 3 \cdot 5 \cdot 7 = 840$. And indeed the computer confirmed that $F(840) = 32$, and that $F(2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11) = 64$. We could suggest a formula for *F(n)!*

It was time to turn the machine off and to prove the conjecture using notions and principles from Number Theory. A simultaneous didactical challenge was how to introduce this investigation to the group of teachers with varied mathematical backgrounds. We will discuss this issue in the concluding section.

3. Formula for *F(n)*

Definition. *Let n be a fixed natural number. Then a and b are said to be congruent modulo n, symbolized by* $a \equiv b \pmod{n}$*, if a - b is divisible by n, i.e.* $a - b = k \cdot n$ *for some integer k.*

Let us note, (see Note 2, Mathematical Appendix.), that any integer *a* can be represented as $a = b + kn$, where $0 \le b \le n-1$. Therefore it is easy to see that if we are interested in

numbers modulo *n*, it is sufficient to consider *0, 1,…, n - 1*. Respectively, the notation $f(x) \equiv 0 (mod\ n)$ means that *f(x)* is divisible by *n* .

In view of the above, Problem 3 can be restated as follows:

Problem 3 (2nd version). *How many solutions does the congruence* $x^2 - 1 \equiv 0 (mod\ n)$ *have?*

The reader is referred to Note 3, Mathematical Appendix for the mathematical background needed to solve this problem.

The essence of the solution lies in the following**:**

Let $n = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$ *be the factorization of n into distinct prime powers. Assume that the congruence* $x \equiv 0 \pmod{p_1^{k_1}}$ *has* t_1 *solutions, the congruence* $x \equiv 0 \pmod{p_2^{k_2}}$ *has* t_2 *solutions,…, the congruence* $x \equiv 0 \pmod{p_s^{k_s}}$ *has* t_s *solutions. Then* $f(x) \equiv 0 \pmod{n}$ *has* $t_1 t_2 ..... t_s$ *solutions.*

Thus, calculation of *F(n)* for a given *n* involves:

(1) Factorization of *n* as a product of powers of distinct prime powers $p_i^{k_i}$ for $1 \le i \le s$;

(2) Counting numbers of solutions of congruences $x^2 - 1 \equiv 0 \pmod{p_i^{k_i}}$ for all such $p_i^{k_i}$;

(3) Multiplying the results.

In this vein, we have:

Lemma 1. *The congruence* $x^2 - 1 \equiv 0 \pmod{p^\alpha}$, *with* α *a natural number and p an odd prime, has only two solutions (mod* p^a*), namely* $x = 1$ *and* $x = p^a - 1$.

Lemma 2. *The congruence* $x^2 - 1 \equiv 0 \pmod{2^\alpha}$ *has:*

(1) One solution $x = 1$ *for* $\alpha = 1$;

(2) Two solutions x =1 and x = 3 for $\alpha = 2$*;*

(3) Four solutions $x=1$, $x=2^{a-1}-1$, $x=2^{a-1}+1$, $x=2^{a}-1$ *for* $\alpha \geq 3$.

For proof of these Lemmas, see Note 4, Mathematical Appendix.

Lemmas 1 and 2 prove the following Corollary:

Corollary. Let $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \ldots p_s^{ks}$.

$$\textit{Then} \quad F(n) = \begin{cases} 2^s & \textit{if} \quad k_0 \leq 1 \\ 2^{s+1} & \textit{if} \quad k_0 = 2 \\ 2^{s+2} & \textit{if} \quad k_0 \geq 3 \end{cases}$$

A final aspect in "hands on" experimentation in the solution of problem 3, was to verify this formula using *Derive* by computing F(n) by this formula, and comparing results with straightforward computations of F(n). The testing is shown in Figure 4, where *PD(n)* gives the list of prime divisors of *n* in increasing order, and the command *ELEMENT(B,k),* gives the *k-th* element of the list *B.*

```
PD(n) := SELECT(PRIME(a) ∧ GCD(a, n) = a, a, 1, n)

                        testing

                    PD(36) = [2, 3]

                    PD(35) = [5, 7]

          F(n) :=
            If ELEMENT(PD(n), 1) ≠ 2
               2^DIM(PD(n))
               If GCD(n, 8) = 8
                  2^(DIM(PD(n)) + 1)
                  If GCD(n, 8) = 4
                     2^DIM(PD(n))
                     If GCD(n, 8) = 2
                        2^(DIM(PD(n)) - 1)

                        testing

                     F(10) = 2

                    F(840) = 32
```

Figure 4: Testing the formula for F(n)

4. Why 2? Open road to the theory of primitive roots

The solution to Problem 3, and the departure in pattern for the prime *p=2*, led naturally to the next realm of investigation, namely:

Why is 2 not like the other prime numbers, both in the number and nature of solutions modulo 2^a as α varies?

The answers require an understanding of the structure; both additive and multiplicative, of Z_n, the set of distinct remainders modulo n, and in particular, the introduction of the notion of a "generator".

Additive generators of Z_n: Whilst the set of integers Z has only one additive generator; *1*, meaning that by adding and subtracting *1*'s, we can obtain any integer, it was noted, by means of the following exercise, that the set Z_n has many additive generators.

Exercise 1. *Show that for any a in Z_n relatively prime to n, the set*

{0, a, 2a, 3a,…, (n-1)a} coincides with Z_n, (meaning that by adding and subtracting a's, we obtain all elements of Z_n).

Remark: This fact is easy seen using *Derive*, *for example for n=9=3^2, a=4*:

[p:=3, α:=2, a:=4]

VECTOR(MOD(a i, p^{α}), i, 0, p^{α} -1) = [0,4,8,3,7,2,6,1,5]*

Multiplicative generators of Z_n: The core of this theory is furnished by Fermat's Little Theorem which was introduced via the following exercise:

Problem 4. For a fixed prime p, s*tudy the values of a^k (modulo p) for different primes p and a in Z_n. Which conclusions can you state?*

After computations for *p=5* (see figure 5) and *p=7,11,* empirical evidence implied that *1* appears in all sequences $a^1, a^2, a^3, a^4, \ldots$ with the maximal period *p-1*.

```
          VECTOR(MOD(2^k, 5), k, 0, 15)
[1, 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3]
          VECTOR(MOD(3^k, 5), k, 0, 15)
[1, 3, 4, 2, 1, 3, 4, 2, 1, 3, 4, 2, 1, 3, 4, 2]
          VECTOR(MOD(4^k, 5), k, 0, 15)
[1, 4, 1, 4, 1, 4, 1, 4, 1, 4, 1, 4, 1, 4, 1, 4]
```

Figure5: residues of a^k modulo 5

In light of the above we could state:

Fermat's Little Theorem. *If p is a prime number and a is an element of* Z_p *(i.e. a is among the numbers 0, 1, …, p-1), then* $a^{p-1} \equiv 1 \pmod{p}$, *i.e.* $a^{p-1} - 1$ *is divisible by p.*

For a reference, see Note 5, Mathematical Appendix.

Another result which was conjectured : if a sequence $a, a^1, a^2, a^3, a^4, \ldots$ is periodic with period of length *p - 1*, then all numbers between *1* and *p-1* occur as distinct powers of *a* *(7,3), (7,5)* etc.

The Multiplicative Structure of Z_{p^α} **:**

Denote by Z_n^* the set of all x in Z_n relatively prime to *n*.

Problem 4 and Fermat's Little Theorem motivated the definition of a *multiplicative* generator of Z_n^*; namely, an element *a* in Z_n^* whose distinct powers $a, a^2, a^3 \ldots,$ yield **the whole of** Z_n^***.** Such numbers are also called **primitive roots** of Z_n^*.

Consider a particular case, *n=p*, for p prime . (For reference as to the existence of primitive roots of Z_p^* for <u>*every*</u> prime p, see Note 6, Mathematical Appendix).

Z_p^* may have several primitive roots, for instance Z_5^* has both 2 and 3 as primitive roots, Z_7^* has 3 and 5 as primitive roots; but not every number is a primitive root, for example, *4* is not a primitive root of either of Z_5^* or Z_7^* .

Problem 5. *For a given* $a \in Z_{p^\alpha}^*$, study the values *of* a^k *modulo n=* p^α .

Testing the case $n = 3^2$ (Figure 6) it was discovered that no element of Z_9 generated all of Z_9 except *0*; thus the *direct* analogue of Fermat's Little Theorem is not true.

```
VECTOR(MOD(2^k, 9), k, 1, 10) = [2, 4, 8, 7, 5, 1, 2, 4, 8, 7]
VECTOR(MOD(3^k, 9), k, 1, 10) = [3, 0, 0, 0, 0, 0, 0, 0, 0, 0]
VECTOR(MOD(4^k, 9), k, 1, 10) = [4, 7, 1, 4, 7, 1, 4, 7, 1, 4]
VECTOR(MOD(5^k, 9), k, 1, 10) = [5, 7, 8, 4, 2, 1, 5, 7, 8, 4]
VECTOR(MOD(6^k, 9), k, 1, 10) = [6, 0, 0, 0, 0, 0, 0, 0, 0, 0]
VECTOR(MOD(7^k, 9), k, 1, 10) = [7, 4, 1, 7, 4, 1, 7, 4, 1, 7]
VECTOR(MOD(8^k, 9), k, 1, 10) = [8, 1, 8, 1, 8, 1, 8, 1, 8, 1]
```

Figure 6: Values *of* a^k *modulo* $n = 3^2$

However, investigating the above results, it was observed that for *a* relatively prime to *9*, all elements of Z_9 relatively prime to *9* were obtained.

Lemma. There exist primitive roots *mod* p^α for odd *p, and every natural number* α .

For proof, see Note 6 , Mathematical Appendix.

At this point we recalled the connection with Problem 3, *and explained in terms of primitive roots*, why $x^2 \equiv 1 (mod\ p^\alpha)$ has precisely two solutions. (for such an explanation, see Note 7, Mathematical Appendix).

Problem 6: Do there exist primitive roots $\bmod 2^\alpha$ **?**

Whilst Z_2^* and $Z_{2^2}^*$ both have primitive roots , namely *1* and *3* respectively, as can easily be verified, it was ***conjectured*** on the basis of the case for odd *p*, that $Z_{2^n}^*$ for $n \geq 3$ does ***not*** have primitive roots, for otherwise the congruence would have two solutions, but it has four.

Exercise 2. *Using Derive, show that* $Z_8^*, Z_{16}^*, Z_{32}^*$ *do not have primitive roots. (Fig. 7)*

```
VECTOR(MOD(3^k, 8), k, 1, 7) = [3, 1, 3, 1, 3, 1, 3]
VECTOR(MOD(5^k, 8), k, 1, 7) = [5, 1, 5, 1, 5, 1, 5]
VECTOR(MOD(7^k, 8), k, 1, 7) = [7, 1, 7, 1, 7, 1, 7]
```

Figure 7: Values of a^k *modulo n = 8 for a in* Z_8^*

This leads naturally to the question: What is the structure of $Z_{2^n}^*$ for $n \geq 3$?

It appears that whilst, as can be seen (see Note 8, Mathematical Appendix) $Z_{2^n}^*$ for $n \geq 3$ does not have primitive roots, $Z_{2^n}^*$ for $n \geq 3$ is generated multiplicatively by **two elements**, meaning that multiplying two certain elements of $Z_{2^n}^*$ and their powers, we can obtain the whole set $Z_{2^n}^*$.

Exercise 3. *Show that 5 and 7 are multiplicative generators of* Z_8^*, *5 and 15 – multiplicative generators of* Z_{16}^*.

Indeed, for Z_8^*, we get $1 \equiv 5^2 \equiv 7^2 \pmod 8$, $3 \equiv 5*7 \pmod 8$, $5 \equiv 5 \pmod 8$, $7 \equiv 7 \pmod 8$.

In the general case (see Note 8, Mathematical Appendix) we get 5 and $2^n\text{-}1 \equiv -1 (mod\ 2^n)$ are multiplicative generators of $Z_{2^n}^*$, and each of elements of $Z_{2^n}^*$ can be represented as $x \equiv \pm 5^k \ (mod\ 2^n)$ for some value of *k*.

To check that for the case of Z_{32}^*, we calculated (Figure 8, note that $7 \equiv -1$), and indeed all the elements of Z_{32}^* were thus obtained.

```
VECTOR(VECTOR(MOD(5^i·(-1)^j, 32), i, 0, 7), j, 0, 1)

[ 1   5  25  29  17  21   9  13 ]
[ 31  27   7   3  15  11  23  19 ]
```

Figure 8: 5 and 7 generate all elements of Z_{32}^*

5. Forward, to Artin's conjecture!

Reflecting on the classical problems of the previous sections and their solutions, it was natural to ask if they connected to a more current area of number theory. We saw that *a=2* was a primitive root for some Z_p^* with prime *p*, for example *p=2,3,5,11*; however, for some *p* values it was not. This begs the following question. For how many primes *p*, will a given fixed number *a* be a primitive root? Specifically, concentrating on the value $a = 2$, the following problem was given to the students:

Problem 7. *Let $\pi(N)$ be the number of primes less than or equal to N, $\nu_2(N)$ be the number of primes less than or equal to N for which 2 is a primitive root. What is the connection between these two numbers for large values of N?*

The following calculations were performed using *Derive* (in Figure 9 **PRIMEPI(N)** simplifies to $\pi(N)$ and the function **PRIMITIVE_ROOT(N)** simplifies to the smallest primitive root modulo *N*).

```
                    PRIMEPI(50000) = 5133
DIM(SELECT(PRIMITIVE_ROOT(n) = 2, n, 2, 50000)) = 1963
                          1963
                          ---- = 0.3824274303
                          5133
                   PRIMEPI(200000) = 17984
DIM(SELECT(PRIMITIVE_ROOT(n) = 2, n, 2, 200000)) = 6766
                          6766
                          ----- = 0.3762233096
                          17984
```

Figure 9: Computing $\nu_2(N)/\pi(N)$

Now the conjecture pointed strongly in the direction of $\nu_2(N) \approx 0.376\,\pi(N)$.

In fact Artin's conjecture is the following: (for further details, see Note 9, Mathematical Appendix.)

Artin's conjecture: *If $a \neq b^n$ with $n > 1$, then $\nu_a(N)) \approx A\ \pi(N)$, where A is Artin's constant, A=0.3739558....*

As a curiosity, it is worth mentioning that such tables up to *N=100,000* were computed manually (!) in 1913 by Cunningham. Additionally, the technique of probability theory, amongst others are involved in Number Theory, and led to Artin's Conjecture as described in Note 9, Mathematical Appendix.

6. A computer led tour into number theory

Clearly, thorough treatment of mathematical problems requires formal background. However, challenging problem-solving situations can motivate people to obtain the knowledge while solving the problems. This is certainly true with Number Theory. Sometimes, if you start to experiment with numbers (with or without the computer) it is almost impossible to stop until a result has been reached: either by some plausible conjecture, or by referring to books. This was the case when we started to explore the solutions of $x^2 - 1 \equiv 0 \pmod{n}$ and the related issues.

The appearance of innovative computational environments, like CAS in schools open new opportunities for performing experimental mathematics before constructing formal proofs. In planning a graduate course for mathematics teachers, *Problem Solving, using CAS*, our intention was that the software would serve not just as a tool for calculation, but rather as a learning and communicative environment. Consequently we emphasized its programming language for exploring problems in various mathematical topics.

Regarding Number theory, we started with Problem 1 dealing with the distribution of prime numbers and leading to the Prime Number Theorem. Being unable to bring the too difficult proof in class, we were presented with an intriguing pedagogical challenge; namely that of bridging between the theorem on the one hand and the computer tools at our disposal on the other. Thus a new task was created, which can also be used by teachers in high school classes. Problem 2 started as a simple exercise of substitutions in the expression $x^2 - 1$. When we ourselves worked on it we realized that the problem could be extended to a tour into the world of Number Theory. Thus the problem was

rephrased as Problem 3: *How many solutions does the congruence* $x^2 - 1 \equiv 0 (\mathrm{mod}\, n)$ *have?* Evidently this problem can be treated experimentally, but the proof requires a fair knowledge in Number Theory. The interesting solution (that we have not found in books), intrigued us and consequently the teachers. As to the question *Why is 2 not like other primes*, here more mathematical background in Number Theory was needed, specifically, the theory of primitive roots. To enable the teachers to work on it experimentally, using the CAS software, a sequence of problems (4-6) and exercises were introduced. Reaching this stage, for didactical reasons we considered it important to implement the knowledge and tools acquired in an additional related topic. We chose to present Artin's conjecture (see Problem 7), which involves primitive roots and is also connected to the Problem 1 that deals with $\pi(N)$, *the number of primes not exceeding N*, from which we started. At this point we concluded our Number Theory didactical tour.

The experimental mathematics was followed by discussion of the theory. We could not develop a rigid discourse in class because the group of teachers was very heterogeneous in terms of mathematical background. Thus we have prepared a mathematical appendix, relevant to the problems, to be used by the learners at their level. This pedagogical solution of compiling a package of problems for investigating with the computer accompanied by a document containing the mathematical background was found helpful during the course, where the teachers were advised individually.

The teachers who participated in the course were graduate students highly motivated to accommodate both the advent of innovative technologies and modern theories of learning in their teaching and research work. For them constructing new knowledge through experimentation, conjectures and investigation was in fact practicing what they preach to

their students. Our enthusiasm and motivation in the preparation of the materials for the course were transparent and for some of the teachers contagious, thus they asked for more explanations on the mathematical appendix and really extended their theoretical knowledge. As mentioned at the beginning of the paper, the first part of the course was the section on number theory. The great involvement in experimenting the problems with the software resulted in fast and good mastery of the CAS environment, easing the work in the next sections. Towards the end of the course the teachers were asked to design CAS-based activities for their classes. Some prepared learning units on prime numbers and their distribution at the intuitive level for junior high school pupils, or for senior high school pupils referring to the PNT. Another unit developed by a teacher had to do with number of divisors of a given number (with or without using the built-in function of the software).

The series of problems described in this paper together with the mathematical appendix can be integrated as a whole or in parts in Number Theory classes. Currently the sequence of problems has been assigned to college students as a project to complement the requirements in a course on Number Theory.

Acknowledgment: The authors are grateful to Professor Ehud De-Shalit and Dr. Giora Mann for their helpful suggestions.

REFERENCES

Books

D.M. Burton, *Elementary Number Theory*, third edition, Wm. C. Brown Publishers, Oxford, 1994

Hua Loo Keng, "Introduction to Number Theory" (Springer-Verlag, Berlin 1982)

V. Klee, S. Wagon, *Old and New Unsolved Problems in Plane Geometry and Number Theory*, MAA, Washington, D.C., 1991

W. J. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley Reading, Massachusetts, 1977

N.H. McCoy, "The Theory of Numbers" (Macmillan, New York 1965)

T. Nagell, "Number Theory" (Chelsea Pub., New York 1964)

D. Shanks, *Solved and Unsolved problems in Number Theory*, Spartan Books, Washington, D.C., 1962

Internet sites

Mathematical Appendix,

http://stwww.weizmann.ac.il/g-math/mathcomp/number-theory.pdf

The Prime Page (An Index of Information on Prime numbers),

http://www.utm.edu/research/primes/

MacTutor: History of Mathematics archive,

http://www-history.mcs.st-and.ac.uk/~history/

Things of interest to Number Theorists,

http://www.math.uga.edu/~ntheory/number_theory.html

Source of information about number theory CAS packages,

http://www.math.uga.edu/~ntheory/N1.html

Biographical Notes

Michael Blinov is due to receive his Ph.D. at the Weizmann Institute of Sciences in 2002, at the Department of Mathematics. His primary research interests lie in the field of mathematical modeling (e.g. cell signal transduction) and dynamical systems,as well as mathematical software, databases and web programming.

Dr. Nurit Zehavi has been working on curriculum development and research in the Science Teaching Department at the Weizmann Institute of Science since 1972. She has coordinated mathematical software development and professional training courses for teachers on using computers in the classroom. Her current research interest is in using computer algebra for teaching mathematics. She is the head of the MathComp project, which was initiated in 1996 with the aim of integrating computer algebra systems into the mathematics curriculum.

Dr. Sarah Black holds a doctorate in Mathematics from Hebrew University Jerusalem. Her research interests lie in the fields of Asymptotic Group Theory and Finite Group Theory. Some of her undergraduate mathematics courses employ computer algebra as a tool for enhancing the understanding of the theoretical material therein.