History of Mathematics #11

1. Before 11 pm, Sunday, April 2. Go to the Forum "Number Theory" and make at least one substantive contribution by 11 pm, Sunday, April 2, and at least one substantive response to others' postings before class on Tuesday, April 4. Write about the following:

   We have encountered elements of number theory throughout the course so far, and again in the current chapter of Dunham. What do mathematicians regard as the domain of "number theory"? In what ways are parts of number theory developed in the K–12 curriculum? What aspects of college level number theory help gain a deeper understanding of pre-college mathematics? Does the development of number theory in the K–12 or K–16 curriculum parallel its historical development or not?

2. Before Tuesday, April 4.

   (a) Read Dunham Chapter 10. Skim Boyer Chapters 22–23.

   (b) Think about the following questions for discussion at the Centra session:

      i. Carefully study the mathematics in chapter 10 of Dunham for good understanding.

      ii. Starting working on the homework problems so that we can talk about them a bit in class.

3. Tuesday, April 4, 7–9 pm. Attend the Centra session to discuss the readings, forum, and comments and questions on the assigned homework due on Saturday.

4. Homework problems due Saturday, April 8, 11 pm, uploaded on the moodle site (preferred method) or submitted to the email address mathhist@ms.uky.edu.

   (a) Although I am not asking you to turn in anything with respect to this first problem, I highly encourage everyone to read *A Mathematician's Apology* by G. H. Hardy. A description can be found in the Wikipedia:

   http://en.wikipedia.org/wiki/A_Mathematician's_Apology

   which includes a link to the book itself:

   www.math.ualberta.ca/~mss/books/A%20Mathematician's%20Apology.pdf.

   Here is one quotation from the book relevant to our current chapter in Dunham and the homework problems to follow:

> But here I must deal with a misconception. It is sometimes suggested that pure mathematicians glory in the uselessness of their work[1], and make it a boast that it has no practical applications. The imputation is usually based on an incautious saying attributed to Gauss, to the effect that, if mathematics is the queen of the sciences, then the theory of numbers is, because of its supreme uselessness, the queen of mathematics—I have never been able to find an exact quotation. I am sure that Gauss's saying (if indeed it be his) has been rather crudely misinterpreted. If the theory of numbers could be employed for any practical and obviously honourable purpose, if it could be turned directly to the furtherance of human happiness or the relief of human suffering, as physiology and even chemistry can, then surely neither Gauss nor any other mathematician would have been so foolish as to decry or regret such applications. But science works for evil as well as for good (and particularly, of course, in time of war); and both Gauss and less mathematicians may be justified in rejoicing that there is one science at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean.

(b) Look up information on "check digits," "error-detecting codes" and "error-correcting codes" and give brief explanations and examples of the following:

i. How is the check digit in ISBN numbers calculated? What kinds of errors can it detect and/or correct?

ii. How is the check digit in UPC codes calculated? What kinds of errors can it detect and/or correct?

iii. What is Verhoeff's check digit method based on the dihedral group D_5? How is the check digit calculated? What kinds of errors can it detect and/or correct? Who uses this method?

(c) Give a brief summary of the meaning of "public-key cryptography" and what this has to do with our current chapter in Dunham. Here is one reference:

www.math.tamu.edu/~boas/courses/math696/public-key-cryptography.html.

[1] [This is Hardy's footnote.] I have been accused of taking this view myself. I once said that 'a science is said to be useful if its development tends to accentuate the existing inequalities in the distribution of wealth, or more directly promotes the destruction of human life', and this sentence, written in 1915, has been quoted (for or against me) several times. It was of course a conscious rhetorical flourish, though one perhaps excusable at the time when it was written.

And here is another, that discusses some of the controversy about publishing the RSA system:

www.livinginternet.com/i/is_crypt_pkc_inv.htm.