BROWN: Math expert helped end WWII

Remembrance Day is Sunday, and it is time to honour those who have fought to keep our country and the world safe.

We all know the role that guns, bombs and tactics played in the Second World War. What I am going to share with you is a story of how mathematician who lived and worked in Canada for most of his life changed the course of the war and likely saved millions of lives.

During the war, the Germans, of course, encoded all of their sensitive military messages, using some sophisticated (and secret) devices (known as Lorenz machines) for encryption.

Those who received the messages could, with the aid of an alphanumeric key (that is, a sequence of letters or numbers) and the machine decode the message quickly. Anyone intercepting the message would be left scratching their heads, trying to make sense of what seeme like random characters.

Some messages from the German high command had been intercepted by British Intelligence, to no effect. A single mistake by a German coding operator led to the sending of two very similar messages with the identical key, and the problem was firmly in the hands of Bletchle Park, the centre for British decryption work.

After months with little progress by the research group, the problem was handed to a 24-year-old mathematician, William Tutte, who had reputation as a problem solver. He began to explore the sequences, looking for patterns — the things mathematics are best prepared to analyze.

Somehow, Tutte noticed patterns in groups of 41 characters, patterns that were likely not random, and from this he inferred that the machine must have had a wheel with 41 teeth. Brilliant!

Further intense study and mathematical deductions led Tutte and his colleagues to determine completely the structure of the internal workings of the Lorenz machine, without having any idea of what the device might look like. Work then began by others to build one of the first electronic computers to carry out the decoding of messages quickly.

The discovery of the decryption process for the Lorenz machines has been called one of the greatest intellectual feats of the war, and it likely hastened the end of the conflict by two years. The number of lives thereby saved is left to the imagination.

After the war, Tutte returned to researching mathematics and was invited to the University of Toronto as a professor. The University of Waterloo, recognizing Tutte's brilliance, lured him away (the story I heard is that they offered him a house).

Tutte wrote exceptional research papers on groundbreaking mathematics in graph theory, the area I work in.

He died in 2002 in Waterloo, at age 84. It's not surprising that the Canadian centre of cryptography (the study of codes) is based there.

On Nov. 11 (which is 11-11 — the double use of prime numbers, which figure so prominently in cryptography), take the time to reflect on the heroes of wars past, and please add a thought for Tutte. His story shows that not only are wars won by blood, sweat and tears but by mathematics, too.

Jason I. Brown is a professor of mathematics at Dalhousie University in Halifax. His research that used mathematics to uncover how the Beatles played the opening chord of A Hard Day's Night has garnered worldwide attention. He is also the author Our Days Are Numbered: How Mathematics Orders Our Lives.

About the Author »

By JASON BROWN

Commenting Policyhttp://thechronicleherald.ca(/node/546)